CONTENTS

About Cisco IOS Software Documentation v
Using Cisco IOS Software xv
On-Demand Routing Commands IP2R-1
RIP Commands IP2R-7
IGRP Commands IP2R-41
OSPF Commands IP2R-65
EIGRP Commands IP2R-151
Integrated IS-IS Commands IP2R-195
BGP Commands IP2R-257
Multiprotocol BGP Extensions for IP Multicast Commands IP2R-453
IP Routing Protocol-Independent Commands IP2R-473

INDEX
About Cisco IOS Software Documentation

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

Documentation Objectives

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

Audience

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

Documentation Organization

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

Documentation Modules

The Cisco IOS documentation modules consist of configuration guides and corresponding command reference publications. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference publication provide complete Cisco IOS command syntax information. Use each configuration guide in conjunction with its corresponding command reference publication.
Figure 1 shows the Cisco IOS software documentation modules.

**Note**

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>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.</td>
</tr>
<tr>
<td>string</td>
<td>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.</td>
</tr>
</tbody>
</table>
Command syntax descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
</tbody>
</table>

Examples use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screen</td>
<td>Examples of information displayed on the screen are set in Courier font.</td>
</tr>
<tr>
<td>boldface screen</td>
<td>Examples of text that you must enter are set in Courier bold font.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Angle brackets enclose text that is not printed to the screen, such as passwords.</td>
</tr>
<tr>
<td>!</td>
<td>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.)</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose default responses to system prompts.</td>
</tr>
</tbody>
</table>

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:


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:


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**

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

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>help</code></td>
<td>Provides a brief description of the help system in any command mode.</td>
</tr>
<tr>
<td><code>abbreviated-command-entry?</code></td>
<td>Provides a list of commands that begin with a particular character string. (No space between command and question mark.)</td>
</tr>
<tr>
<td><code>abbreviated-command-entry&lt;Tab&gt;</code></td>
<td>Completes a partial command name.</td>
</tr>
<tr>
<td><code>?</code></td>
<td>Lists all commands available for a particular command mode.</td>
</tr>
<tr>
<td><code>command ?</code></td>
<td>Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
</table>
| Router> enable                 | Enter the `enable` command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to Router#.
| Password: <password>           |                                                                         |
| Router#                        |                                                                         |
| Router# configure terminal     | 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)#. |
| Enter configuration commands, one per line. End with CNTL/Z. |                                                                         |
| Router(config)#               |                                                                         |
| Router(config)# interface serial ? | Enter interface configuration mode by specifying the serial interface that you want to configure using the `interface serial` global configuration command. |
| <0-6> Serial interface number | 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. |
| Router(config)# interface serial 4 ? |                                                                         |
| /                             |                                                                         |
| Router(config)# interface serial 4/ ? |                                                                         |
| <0-3> Serial interface number | You are in interface configuration mode when the prompt changes to Router(config-if)#. |
| Router(config)# interface serial 4/0 |                                                                         |
| Router(config-if)#            |                                                                         |
Table 2  How to Find Command Options (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# ?</td>
<td>Interface configuration commands:</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td>ip</td>
<td>Interface Internet Protocol config commands</td>
</tr>
<tr>
<td>keepalive</td>
<td>Enable keepalive</td>
</tr>
<tr>
<td>lan-name</td>
<td>LAN Name command</td>
</tr>
<tr>
<td>llc2</td>
<td>LLC2 Interface Subcommands</td>
</tr>
<tr>
<td>load-interval</td>
<td>Specify interval for load calculation for an interface</td>
</tr>
<tr>
<td>locaddr-priority</td>
<td>Assign a priority group</td>
</tr>
<tr>
<td>logging</td>
<td>Configure logging for interface</td>
</tr>
<tr>
<td>loopback</td>
<td>Configure internal loopback on an interface</td>
</tr>
<tr>
<td>mac-address</td>
<td>Manually set interface MAC address</td>
</tr>
<tr>
<td>mls</td>
<td>mls router sub/interface commands</td>
</tr>
<tr>
<td>mpoa</td>
<td>MPOA interface configuration commands</td>
</tr>
<tr>
<td>mtu</td>
<td>Set the interface Maximum Transmission Unit (MTU)</td>
</tr>
<tr>
<td>netbios</td>
<td>Use a defined NETBIOS access list or enable name-caching</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>nrzi-encoding</td>
<td>Enable use of NRZI encoding</td>
</tr>
<tr>
<td>ntp</td>
<td>Configure NTP</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td>Router(config-if)#</td>
<td>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.</td>
</tr>
<tr>
<td>ip ?</td>
<td>Enter the command that you want to configure for the interface. This example uses the ip command.</td>
</tr>
<tr>
<td></td>
<td>Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</td>
</tr>
</tbody>
</table>

T able 2 How to Find Command Options (continued)
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 an On-Demand Routing (ODR) process on a Cisco router, use the `router odr` command in global configuration mode. To disable the ODR process, use the `no` form of this command.

```
router odr
no router odr
```

#### Syntax Description

This command has no arguments or keywords

#### Defaults

No default behavior or values

#### Command Modes

Global configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The `router odr` command is used to configure a router as an ODR hub router to dynamically accept routes from stub peers. ODR provides IP routing with minimal configuration requirements. The overhead of dynamic routing protocol is avoided without incurring the configuration and management overhead of static routing.

The ODR process maintains a routing table, which is populated with information learned from ODR stub peers. Cisco Discovery Protocol (CDP) must be enabled on the hub router and stub peers. ODR timing values should be tuned based on the number of peers and the speed of the links in your network. Route filtering should be applied consistently.

#### Examples

In the following example, an ODR process is enabled, a distribution list is configured to filter routes learned from ODR stub peers, and redistribution statement is configured under the Open Shortest Path First (OSPF) routing process:

```
Router(config)# access-list 101 permit ip host 10.0.0.1 192.168.1.0 0.0.0.255
Router(config)# access-list 101 permit ip 10.0.10.2 255.0.0.0 192.168.2.0 0.0.0.255
Router(config)#
Router(config)# router odr
Router(config-router)# distribute-list 101 in
Router(config-router)# exit
Router(config-router)# router ospf 1
Router(config-router)# redistribute odr subnets
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdp timer</td>
<td>Specifies how often the Cisco IOS software sends CDP updates.</td>
</tr>
<tr>
<td>distance (IP)</td>
<td>Defines an administrative distance.</td>
</tr>
<tr>
<td>distribute-list in (IP)</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>distribute-list out (IP)</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>maximum-paths</td>
<td>Controls the maximum number of parallel routes an IP routing protocol can support.</td>
</tr>
<tr>
<td>timers basic (ODR)</td>
<td>Adjusts ODR network timers.</td>
</tr>
</tbody>
</table>
timers basic (ODR)

To adjust On-Demand Routing (ODR) network timers, use the **timers basic** command in router configuration mode. To restore default ODR timer values, use the **no** form of this command.

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

no timers basic
```

### Syntax Description

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

### Defaults

ODR uses the following default values if this command is not configured or if the no form of this command is entered:

- **update**: 90 seconds
- **invalid**: 270 seconds
- **holddown**: 280 seconds
- **flush**: 630 seconds
- **sleeptime**: 0 milliseconds

### Command Modes

- Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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 are displayed in the output of the `show ip protocols` EXEC command. The relationships of the various timers should be preserved as described in the syntax description table.

Examples
In the following example, updates are configured to be broadcast every 5 seconds. If a reply is not received from a peer within 15 seconds, the route is declared unusable. Further information the dead peer is suppressed for an additional 15 seconds. At the end of the suppression period, the route is flushed from the routing table.

```
Router(config)# router odr
Router(config-router)# timers basic 5  15  15  30
Router(config-router)# end
```

Note
When configuring a short update period, you run the risk of congesting slow-speed serial lines; however, this is less of a concern on high-speed links, such as Fast Ethernet, Gigabit Ethernet, and T1-rate serial links. 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdp timer</td>
<td>Specifies how often the Cisco IOS software sends CDP updates,</td>
</tr>
<tr>
<td>router odr</td>
<td>Configures an ODR process on a Cisco router.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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. The metric of redistributed connected and static routes is set to 0.

Command Modes

Router configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.

```
Note
When enabled, the `default-metric` command applies a metric value of 0 to redistributed connected routes. The `default-metric` command does not override metric values that are applied with the `redistribute` command.
```

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
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.

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-number</code>, <code>interface-type</code>, and <code>interface-number</code> arguments were added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>prefix-list-name</code> argument was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>
Usage Guidelines

This command is not supported in Intermediate System-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:

```plaintext
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:

```plaintext
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:

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>distribute-list out (RIP, IGRP, EIGRP)</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-number</code> argument was added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>prefix-list-name</code> argument was added.</td>
</tr>
<tr>
<td>12.0(?)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>distribute-list in (RIP, IGRP, EIGRP)</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip protocols</td>
<td>Displays the parameters and current state of the active routing protocol process.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output-delay</td>
<td>Changes interpacket delay for RIP updates sent.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key chain</td>
<td>Enables authentication for routing protocols.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>text</td>
<td>Clear text authentication.</td>
</tr>
<tr>
<td>md5</td>
<td>Keyed Message Digest 5 (MD5) authentication.</td>
</tr>
</tbody>
</table>

**Defaults**

Clear text authentication is provided for RIP packets.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rip authentication key-chain</td>
<td>Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.</td>
</tr>
<tr>
<td>key chain</td>
<td>Enables authentication for routing protocols.</td>
</tr>
</tbody>
</table>
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.

```plaintext
ip rip receive version [1] [2]
no ip rip receive version
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(Optional) Accepts only RIP Version 1 packets on the interface.</td>
</tr>
<tr>
<td>2</td>
<td>(Optional) Accepts only RIP Version 2 packets on the interface.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

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

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

```plaintext
ip rip receive version 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key chain</td>
<td>Enables authentication for routing protocols.</td>
</tr>
<tr>
<td>ip rip authentication key-chain</td>
<td>Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.</td>
</tr>
<tr>
<td>ip rip send version</td>
<td>Specifies a RIP version to send on an interface basis.</td>
</tr>
<tr>
<td>version</td>
<td>Specifies a RIP version used globally by the router.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>1</th>
<th>(Optional) Sends only RIP Version 1 packets out the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>(Optional) Sends only RIP Version 2 packets out the interface.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip rip receive version</code></td>
<td>Specifies a RIP version to receive on an interface basis.</td>
</tr>
<tr>
<td><code>version</code></td>
<td>Specifies a RIP version used globally by the router.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show ip rip database</td>
<td>Displays the contents of the RIP private database when triggered extensions to RIP are enabled.</td>
</tr>
</tbody>
</table>
**ip rip v2-broadcast**

To allow Routing Information Protocol (RIP) Version 2 update packets to be sent as broadcast packets instead of multicast packets, use the `rip v2-broadcast` command in interface configuration mode. To disable the broadcast of IP RIP Version 2 update packets that are sent as broadcast packets, use the `no` form of this command.

```
ip rip v2-broadcast

no ip rip v2-broadcast
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command is disabled by default. Unless the `ip rip v2-broadcast` command is entered, RIP Version 2 update packets are sent as multicast packets.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(5)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip rip v2-broadcast` command to broadcast RIP Version 2 broadcast updates to hosts that do not listen to multicast broadcasts. Version 2 updates (requests and responses) will be sent to the IP broadcast address 255.255.255.255 instead of the IP multicast address 244.0.0.9.

In order to reduce unnecessary load on those hosts that are not listening to RIP Version 2 broadcasts, the system uses an IP multicast address for periodic broadcasts. The IP multicast address is 244.0.0.9.

**Note**

It is not necessary to configure Internet Group Management Protocol (IGMP) because the periodic broadcasts are interrouter messages that are not forwarded.

**Examples**

The following example configures Version 2 IP broadcast updates on RIP Ethernet interface 3/1:

```
Router(config) interface ethernet3/1
Router(config-if) ip address 172.1.1.1 255.255.255.0
Router(config-if) ip rip v2-broadcast

Router(config-if) router rip
Router(config-if) version 2
Router(config-if) network 172.0.0.0
```

Enter `debug ip rip` command to verify that RIP Version 2 IP broadcast updates are being sent to the IP broadcast address 255.255.255 instead of IP multicast address 244.0.0.9:
Router# debug ip rip
14:41:59: RIP: sending v2 update to 255.255.255.255 via Ethernet3/1 (172.1.1.1)

If the `ip rip v2-broadcast` command has not been entered, the output from the `debug ip rip` command verifies that the RIP Version 2 IP broadcast updates are being sent to the IP multicast address 244.0.0.9:

Router# debug ip rip
15:45:16: RIP: sending v2 update to 244.0.0.9 via Ethernet3.1 (172.1.1.1)

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip rip</td>
<td>Displays information on RIP routing transactions.</td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor (RIP)</td>
<td>Defines a neighboring router with which to exchange routing information.</td>
</tr>
</tbody>
</table>
ip summary-address rip

To configure a summary aggregate address under an interface for the Routing Information Protocol (RIP), use the `ip summary-address rip` command in interface configuration mode. To disable summarization of the specified address or subnet, 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

RIP automatically summarizes to classful network boundaries.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The `ip summary-address rip` command is used to summarize an address or subnet under a specific interface. RIP automatically summarizes to classful network boundaries. Only one summary address can be configured for each classful subnet.

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.
```

```
interface Ethernet1
 ip address 10.1.1.1 255.255.255.0
 ip summary-address rip 10.2.0.0 255.255.0
 exit

router rip
 network 10.0.0.0
end
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>auto-summary (RIP)</strong></td>
<td>Restores the default behavior of automatic summarization of subnet routes into network-level routes.</td>
</tr>
<tr>
<td><strong>ip split-horizon (RIP)</strong></td>
<td>Enables the split horizon mechanism.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive-interface</td>
<td>Disables sending routing updates on an interface.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the network of directly connected networks.</td>
</tr>
</tbody>
</table>

### Defaults

No networks are specified.

### Command Modes

Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>router rip</code></td>
<td>Configures the RIP routing process.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-number</td>
<td>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.</td>
</tr>
<tr>
<td>access-list-name</td>
<td>Standard access list name to be applied.</td>
</tr>
<tr>
<td>in</td>
<td>Applies the access list to incoming metrics.</td>
</tr>
<tr>
<td>out</td>
<td>Applies the access list to outgoing metrics.</td>
</tr>
<tr>
<td>offset</td>
<td>Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.</td>
</tr>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type to which the offset list is applied.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Interface number to which the offset list is applied.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>10.3</td>
<td>The interface-type and interface-number arguments were added.</td>
</tr>
<tr>
<td>11.2</td>
<td>The access-list-name argument was added.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>delay</th>
<th>Delay (in milliseconds) between packets in a multiple-packet RIP update. The range is from 8 to 50 milliseconds. The default is no delay.</th>
</tr>
</thead>
</table>

**Defaults**

0 milliseconds

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

```
router rip
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>network (RIP)</code></td>
<td>Specifies a list of networks for the RIP process.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>(Optional) Address about which routing information should be displayed.</td>
</tr>
<tr>
<td>mask</td>
<td>Argument for the subnet mask. The subnet mask must also be specified if the IP address argument is entered.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
10.0.0.0/8    auto-summary
10.11.0.0/16  int-summary
10.11.11.0/24 directly connected, Ethernet3
10.11.12.0/24 directly connected, Ethernet4
10.11.10.0/24 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16 auto-summary</td>
<td>Summary address entry.</td>
</tr>
<tr>
<td>10.11.1.0/24 directly connected, Ethernet0</td>
<td>Directly connected entry for Ethernet 0.</td>
</tr>
<tr>
<td>172.19.65.0/24 [1] via 172.19.70.36, 00:00:17, Serial0</td>
<td>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 interface 0, 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.</td>
</tr>
<tr>
<td>172.19.65.0/24 [2] via 172.19.67.38, 00:00:25, Serial1</td>
<td></td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rip triggered</td>
<td>Enables triggered extensions of RIP.</td>
</tr>
<tr>
<td>ip summary-address rip</td>
<td>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.</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>Displays the parameters and current state of the active routing protocol process.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>update</td>
<td>Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.</td>
</tr>
<tr>
<td>invalid</td>
<td>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.</td>
</tr>
<tr>
<td>holddown</td>
<td>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.</td>
</tr>
<tr>
<td>flush</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Defaults**

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

**Command Modes**

- Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Specifies RIP Version 1.</td>
</tr>
<tr>
<td>2</td>
<td>Specifies RIP Version 2.</td>
</tr>
</tbody>
</table>

### Defaults

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

### Command Modes

Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip rip receive version</code></td>
<td>Specifies a RIP version to receive on an interface basis.</td>
</tr>
<tr>
<td><code>ip rip send version</code></td>
<td>Specifies a RIP version to send on an interface basis.</td>
</tr>
<tr>
<td><code>show ip protocols</code></td>
<td>Displays the parameters and current state of the active routing protocol process.</td>
</tr>
</tbody>
</table>
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**

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

**Defaults**

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

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

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.

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
**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
d no distribute-list {access-list-number | prefix prefix-list-name [gateway prefix-list-name]} in
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-number</code></td>
<td>Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.</td>
</tr>
<tr>
<td><code>prefix prefix-list-name</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>gateway prefix-list-name</code></td>
<td>(Optional) Name of the prefix list to be applied to the gateway of the prefix being updated.</td>
</tr>
<tr>
<td><code>in</code></td>
<td>Applies the access list to incoming routing updates.</td>
</tr>
<tr>
<td><code>interface-type</code></td>
<td>(Optional) Interface type.</td>
</tr>
<tr>
<td><code>interface-number</code></td>
<td>(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.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-number</code>, <code>interface-type</code>, and <code>interface-number</code> arguments were added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>prefix-list-name</code> argument was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

This command is not supported in Intermediate System-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:

```plaintext
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:

```plaintext
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:

```plaintext
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list (IP extended)</code></td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td><code>distribute-list out (RIP, IGRP, EIGRP)</code></td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td><code>ip prefix-list</code></td>
<td>Creates an entry in a prefix list.</td>
</tr>
<tr>
<td><code>redistribute (IP)</code></td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-number</code></td>
<td>Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.</td>
</tr>
<tr>
<td><code>prefix prefix-list-name</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>gateway prefix-list-name</code></td>
<td>(Optional) Name of the prefix list to be applied to the gateway of the prefix being updated.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Applies the access list to outgoing routing updates.</td>
</tr>
<tr>
<td><code>interface-name</code></td>
<td>(Optional) Name of a particular interface.</td>
</tr>
<tr>
<td><code>routing-process</code></td>
<td>(Optional) Name of a particular routing process, or the keyword <code>static</code> or <code>connected</code>.</td>
</tr>
<tr>
<td><code>as-number</code></td>
<td>(Optional) Autonomous system number.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-number</code> argument was added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>prefix-list-name</code> argument was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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.
IGRP Commands

**distribute-list out (RIP, IGRP, EIGRP)**

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:

```conf
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>distribute-list in (RIP, IGRP, EIGRP)</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>network (IGRP)</code></td>
<td>Specifies a list of networks for the IGRP or EIGRP routing process.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric maximum-hops</td>
<td>Causes the IP routing software to advertise as unreachable those routes with a hop count higher than is specified by the command (IGRP only).</td>
</tr>
<tr>
<td>metric weights (EIGRP)</td>
<td>Allows the tuning of the IGRP or EIGRP metric calculation.</td>
</tr>
<tr>
<td>timers basic (IGRP)</td>
<td>Adjusts IGRP network timers.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric holddown</td>
<td>Keeps new IGRP routing information from being used for a certain period of time.</td>
</tr>
<tr>
<td>metric weights (EIGRP)</td>
<td>Allows the tuning of the IGRP or EIGRP metric calculations.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tos</td>
<td>Type of service must always be zero.</td>
</tr>
<tr>
<td>k1, k2, k3, k4, k5</td>
<td>Constants that convert an IGRP or EIGRP metric vector into a scalar quantity.</td>
</tr>
</tbody>
</table>

**Defaults**

- **tos**: 0
- **k1**: 1
- **k2**: 0
- **k3**: 1
- **k4**: 0
- **k5**: 0

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

\[
\text{metric} = [k1 \times \text{bandwidth} + (k2 \times \text{bandwidth})/(256 - \text{load}) + k3 \times \text{delay}]
\]

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

\[
\text{metric} = \text{metric} \times [k5/(\text{reliability} + k4)]
\]

Bandwidth is inverse minimum bandwidth of the path in BPS scaled by a factor of \(2.56 \times 10^{12}\). 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

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Delay</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satellite</td>
<td>5120</td>
<td>5120 (500 megabits)</td>
</tr>
<tr>
<td>Ethernet</td>
<td>25600</td>
<td>256000 (10 megabits)</td>
</tr>
<tr>
<td>1.544 Mbps</td>
<td>512000</td>
<td>1,657,856 bits</td>
</tr>
<tr>
<td>64 kbps</td>
<td>512000</td>
<td>40,000,000 bits</td>
</tr>
<tr>
<td>56 kbps</td>
<td>512000</td>
<td>45,714,176 bits</td>
</tr>
<tr>
<td>10 kbps</td>
<td>512000</td>
<td>256,000,000 bits</td>
</tr>
<tr>
<td>1 kbps</td>
<td>512000</td>
<td>2,560,000,000 bits</td>
</tr>
</tbody>
</table>

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:

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

### Related Commands

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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of a peer router with which routing information will be exchanged.</td>
</tr>
</tbody>
</table>

### Defaults

No neighboring routers are defined.

### Command Modes

Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive-interface</td>
<td>Disables sending routing updates on an interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router igrp</td>
<td>Configures the IGRP routing process.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>10.3</td>
<td>The <code>interface-type</code> and <code>interface-number</code> arguments were added.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-name</code> argument was added.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network (IGRP)</td>
<td>Specifies a list of networks for the IGRP or EIGRP routing process.</td>
</tr>
</tbody>
</table>
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**

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

**Defaults**

No metric will be set in the route map.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another.</td>
</tr>
</tbody>
</table>
**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>update</code></td>
<td>Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 90 seconds.</td>
</tr>
<tr>
<td><code>invalid</code></td>
<td>Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <code>update</code> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters <code>holddown</code> state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 270 seconds.</td>
</tr>
<tr>
<td><code>holddown</code></td>
<td>Interval (in seconds) during which routing information regarding better paths is suppressed. It should be at least three times the value of the <code>update</code> 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 <code>holddown</code> expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 280 seconds.</td>
</tr>
<tr>
<td><code>flush</code></td>
<td>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 <code>invalid</code> argument and the <code>holddown</code> argument. If it is less than this sum, the proper <code>holddown</code> interval cannot elapse, which results in a new route being accepted before the <code>holddown</code> interval expires. The default is 630 seconds.</td>
</tr>
<tr>
<td><code>sleeptime</code></td>
<td>(Optional) Interval (in milliseconds) for postponing routing updates in the event of a flash update. The value of the <code>sleeptime</code> argument should be less than the <code>update</code> value. If the <code>sleeptime</code> value is greater than the <code>update</code> value, routing tables will become unsynchronized. The default is 0 milliseconds.</td>
</tr>
</tbody>
</table>

### Defaults

- `update`: 90 seconds
- `invalid`: 270 seconds
- `holddown`: 280 seconds
- `flush`: 630 seconds
- `sleeptime`: 0 milliseconds

### Command Modes

Router configuration
IGRP Commands

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip protocols</code></td>
<td>Displays the parameters and current state of the active routing protocol process.</td>
</tr>
</tbody>
</table>
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.

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>variance (IGRP)</td>
<td>Controls load balancing in an EIGRP and IGRP internetwork.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0</td>
<td>The <code>message-digest</code> keyword was added.</td>
</tr>
</tbody>
</table>

**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 adedefgh
!
interface ethernet 1
  ip address 10.56.0.201 255.255.0.0
  ip ospf authentication-key ijklmnop
!
routerr 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>area default-cost</code></td>
<td>Specifies a cost for the default summary route sent into a stub area.</td>
</tr>
<tr>
<td><code>area stub</code></td>
<td>Defines an area as a stub area.</td>
</tr>
<tr>
<td><code>ip ospf authentication-key</code></td>
<td>Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.</td>
</tr>
<tr>
<td><code>ip ospf message-digest-key</code></td>
<td>Enables OSPF MD5 authentication.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>area authentication</td>
<td>Enables authentication for an OSPF area.</td>
</tr>
<tr>
<td></td>
<td>area stub</td>
<td>Defines an area as a stub area.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(15)S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>area-id</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>no-redistribution</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>default-information-originate</code></td>
<td>(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).</td>
</tr>
<tr>
<td><code>metric</code></td>
<td>OSPF default metric.</td>
</tr>
<tr>
<td><code>metric-type</code></td>
<td>OSPF metric type for default routes.</td>
</tr>
<tr>
<td><code>no-summary</code></td>
<td>(Optional) Allows an area to be a not-so-stubby area but not have summary routes injected into it.</td>
</tr>
</tbody>
</table>

**Defaults**

No NSSA area is defined.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>area-id</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>IP address.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>IP address mask.</td>
</tr>
<tr>
<td><code>advertise</code></td>
<td>(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).</td>
</tr>
<tr>
<td><code>not-advertise</code></td>
<td>(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.</td>
</tr>
<tr>
<td><code>cost cost</code></td>
<td>(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.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2</td>
<td>The <code>cost cost</code> keyword and argument were added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area authentication</td>
<td>Enables authentication for an OSPF area.</td>
</tr>
<tr>
<td>area default-cost</td>
<td>Specifies a cost for the default summary route sent into a stub area.</td>
</tr>
<tr>
<td>area nssa</td>
<td>Configures an area as an NSSA.</td>
</tr>
<tr>
<td>area stub</td>
<td>Defines an area as a stub area.</td>
</tr>
<tr>
<td>area virtual-link</td>
<td>Defines an OSPF virtual link.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>Identifier for the stub area; either a decimal value or an IP address.</td>
</tr>
<tr>
<td>no-summary</td>
<td>(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.</td>
</tr>
</tbody>
</table>

**Defaults**

No stub area is defined.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area authentication</td>
<td>Enables authentication for an OSPF area.</td>
</tr>
<tr>
<td>area default-cost</td>
<td>Specifies a cost for the default summary route sent into a stub area.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>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.</td>
</tr>
<tr>
<td>router-id</td>
<td>Router ID associated with the virtual link neighbor. The router ID appears in the <code>show ip ospf</code> 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.</td>
</tr>
<tr>
<td>authentication</td>
<td>(Optional) Specifies authentication type.</td>
</tr>
<tr>
<td>message-digest</td>
<td>(Optional) Specifies that message-digest authentication is used.</td>
</tr>
<tr>
<td>null</td>
<td>(Optional) No authentication is used. Overrides password or message-digest authentication if configured for the area.</td>
</tr>
<tr>
<td>hello-interval seconds</td>
<td>(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.</td>
</tr>
<tr>
<td>retransmit-interval seconds</td>
<td>(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.</td>
</tr>
<tr>
<td>transmit-delay seconds</td>
<td>(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.</td>
</tr>
<tr>
<td>dead-interval seconds</td>
<td>(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.</td>
</tr>
</tbody>
</table>
**area virtual-link**

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0</td>
<td>The <code>message-digest-key key-id md5 key</code> keywords and arguments were added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>authentication</code>, <code>message-digest</code>, and <code>null</code> keywords were added.</td>
</tr>
</tbody>
</table>

**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.

For Cisco IOS Release 12.2 and later releases, authentication type now is specified on a per-interface basis, rather than on a per-area basis, per RFC 2178. For backward compatibility, authentication type for an area is still supported. If the authentication type is not specified for an interface, the interface will use the authentication type that was specified for the area. If no authentication type has been specified for the area, the area default is null authentication.

**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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area authentication</td>
<td>Enables authentication for an OSPF area.</td>
</tr>
<tr>
<td>service password-encryption</td>
<td>Encrypts passwords.</td>
</tr>
<tr>
<td>show ip ospf</td>
<td>Displays general information about OSPF routing processes.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>reference-bandwidth ref-bw</code></td>
<td>Rate in Mbps (bandwidth). The range is from 1 to 4294967; the default is 100.</td>
</tr>
</tbody>
</table>

**Defaults**

100 Mbps

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ospf cost</code></td>
<td>Explicitly specifies the cost of sending a packet on an interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pid</td>
<td>(Optional) Process ID.</td>
</tr>
<tr>
<td>process</td>
<td>Reset OSPF process.</td>
</tr>
<tr>
<td>redistribution</td>
<td>Clear OSPF route redistribution.</td>
</tr>
<tr>
<td>counters</td>
<td>OSPF counters.</td>
</tr>
<tr>
<td>neighbor</td>
<td>(Optional) Neighbor statistics per interface.</td>
</tr>
<tr>
<td>neighbor-interface</td>
<td>(Optional) Neighbor interface.</td>
</tr>
<tr>
<td>neighbor-id</td>
<td>(Optional) Neighbor ID.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>always</code></td>
<td>(Optional) Always advertises the default route regardless of whether the software has a default route.</td>
</tr>
<tr>
<td><code>metric metric-value</code></td>
<td>(Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the <code>default-metric</code> router configuration command, the default metric value is 1. The value used is specific to the protocol.</td>
</tr>
<tr>
<td><code>metric-type type-value</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>route-map map-name</code></td>
<td>(Optional) Routing process will generate the default route if the route map is satisfied.</td>
</tr>
</tbody>
</table>

### Defaults

This command is disabled by default.

### Command Modes

Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 address 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:

```
routing ospf 109
redistribute igrp 108 metric 100 subnets
default-information originate metric 100 metric-type 1
```
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. The metric of redistributed connected and static routes is set to 0.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**Note**

When enabled, the `default-metric` command applies a metric value of 0 to redistributed connected routes. The `default-metric` command does not override metric values that are applied with the `redistribute` command.

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>redistribute (IP)</code></td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
**discard-route**

To reinstall either an external or internal discard route that was previously removed, use the `discard-route` command in router configuration mode. To remove either an external or internal discard route, use the `no` form of this command.

```
discard-route [external | internal]
```

```
o discard-route [external | internal]
```

**Syntax Description**

- **external** (Optional) Reinstalls the discard route entry for redistributed summarized routes on an Autonomous System Boundary Router (ASBR).
- **internal** (Optional) Reinstalls the discard-route entry for summarized internal routes on the Area Border Router (ABR).

**Defaults**

External and internal discard route entries are installed.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

External and internal discard route entries are installed in routing tables by default. During route summarization, routing loops may occur when data is sent to a nonexisting network that appears to be a part of the summary, and the router performing the summarization has a less specific route (pointing back to the sending router) for this network in its routing table. To prevent the routing loop, a discard route entry is installed in the routing table of the ABR or ASBR.

If for any reason you do not want to use the external or internal discard route, remove the discard route by entering the no discard-route command with either the external or internal keyword.

**Examples**

The following display shows the discard route functionality installed by default. When external or internal routes are summarized, a summary route to Null0 will appear in the router output from the `show ip route` command. See the router output lines that appear in bold font:

```
Router# show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
O - ODR, P - periodic downloaded static route
Gateway of last resort is not set

172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
C 172.16.0.128/25 is directly connected, Loopback1
O 172.16.0.0/24 is a summary, 00:00:14, Null0
C 172.16.0.0/25 is directly connected, Loopback0
172.31.0.0/24 is variably subnetted, 3 subnets, 2 masks
C 172.31.0.128/25 is directly connected, Loopback3
O 172.31.0.0/24 is a summary, 00:00:02, Null0
C 172.31.0.0/25 is directly connected, Loopback2
C 192.168.0.0/24 is directly connected, Ethernet0/0

RouterB# show ip route ospf

172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
O 172.16.0.0/24 is a summary, 00:00:29, Null0
172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
O 201.0.0.0/24 is a summary, 00:00:17, Null0

When the no discard-route command with the internal keyword is entered, notice the following route change, indicated by the router output lines that appear in bold font:

RouterB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)# router ospf 1
RouterB(config-router)# no discard-route internal
RouterB(config-router)# end

RouterB# show ip route ospf

172.31.0.0/24 is variably subnetted, 3 subnets, 2 masks
O 172.16.0.0/24 is a summary, 00:04:14, Null0

Next, the no discard-route command with the external keyword is entered to remove the external discard route entry:

RouterB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)# router ospf 1
RouterB(config-router)# no discard-route external
RouterB(config-router)# end

The following router output from the show running-config command confirms that both the external and internal discard routes have been removed from the routing table of RouterB. See the router output lines that appear in bold font:

RouterB# show running-config
Building configuration...

Current configuration : 1114 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
.
.
router ospf 1
  log-adjacency-changes
  no discard-route external
  no discard-route internal
  area 1 range 172.16.0.0 255.255.255.0
  summary-address 172.31.0.0 255.255.255.0
  redistribute rip subnets
  network 192.168.0.0 0.0.0.255 area 0
  network 172.16.0.0 0.0.0.255 area 1
!

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip route</td>
<td>Displays the current state of the routing table.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1(14)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>distance (IP)</td>
<td>Defines an administrative distance.</td>
</tr>
</tbody>
</table>
domain-tag

To set the Open Shortest Path First (OSPF) domain tag value for Type-5 or Type-7 link-state advertisements (LSAs) when OSPF is used as a protocol between a provider edge (PE) router and customer edge (CE) router, use the **domain-tag** command in router configuration mode. To reinstate the default tag value, use the **no** form of this command.

**domain-tag tag-value**

**no domain-tag tag-value**

**Syntax Description**

| tag-value | Tag value. A 32-bit value entered in decimal format. The default value is calculated based on the Border Gateway Protocol (BGP) autonomous system (AS) number of the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) backbone. The four highest bits are set to 1101 according to RFC 1745. The lowest 16 bits map the BGP AS number of the MPLS VPN backbone. If a user specifies the tag-value, the value does not have to follow any particular format. |

**Defaults**

The default value is calculated based on the BGP autonomous system number of the MPLS VPN backbone. The four highest bits are set to 1101 according to RFC 1745. The lowest 16 bits map the BGP autonomous system number of the MPLS VPN backbone.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(7)</td>
<td>The command was introduced.</td>
</tr>
<tr>
<td>12.1(7)E</td>
<td>The command was integrated into Cisco IOS Release 12.1(7)E.</td>
</tr>
<tr>
<td>12.1(7)EC</td>
<td>The command was integrated into Cisco IOS Release 12.1(7)EC.</td>
</tr>
<tr>
<td>12.0(17)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(17)ST.</td>
</tr>
<tr>
<td>12.2(2)B</td>
<td>The command was integrated into Cisco IOS Release 12.2(2)B.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>The command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When OSPF is used between a PE router and a CE router, BGP routes that come from the MPLS backbone are redistributed to OSPF. These redistributed routes can be announced in Type-3, Type-5, or Type-7 LSAs. If the redistribution of the BGP routes results in Type-5 or Type-7 LSAs, the External Route Tag will be set to the value of the tag. If another PE router receives a Type-5 or Type-7 LSA with an External Route Tag equal to the set tag value, it will ignore the LSA, therefore preventing the redistributed routes that originated from the MPLS backbone from returning via some other location on the MPLS backbone.
Examples

The following example configures the tag value 777:

Router(config)# router ospf 10 vrf grc
Router(config-router)# domain-tag 777

The `show ip ospf database` command is entered to verify that the tag value 777 has been applied to the External Route Tag:

Router# show ospf database external 192.168.50.1

```
OSPF Router with ID (192.168.239.66) (Process ID 10)

Type-5 AS External Link States

LS age: 18
Options: (No TOS-capability, DC)
S Type: AS External Link
Link State ID: 192.168.238.1 (External Network Number)
Advertising Router: 192.168.239.66
LS Seq Number: 80000002
Checksum: 0xDAB0
Length: 36
Network Mask: /32

Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 777

OSPF Router with ID (198.168.237.56) (Process ID 1)
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ospf database</td>
<td>Displays lists of information related to the OSPF database for a specific router.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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]
```

```
oip ospf authentication
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>message-digest</td>
<td>(Optional) Specifies that message-digest authentication will be used.</td>
</tr>
<tr>
<td>null</td>
<td>(Optional) No authentication is used. Useful for overriding password or message-digest authentication if configured for an area.</td>
</tr>
</tbody>
</table>

**Defaults**

The area default is no authentication (null authentication).

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area authentication</td>
<td>Enables authentication for an OSPF area.</td>
</tr>
<tr>
<td>ip ospf authentication-key</td>
<td>Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.</td>
</tr>
<tr>
<td>ip ospf message-digest-key</td>
<td>Enables OSPF MD5 authentication.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>password</strong></td>
<td>Any continuous string of characters that can be entered from the keyboard up to 8 bytes in length.</td>
</tr>
</tbody>
</table>

**Defaults**

No password is specified.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area authentication</td>
<td>Enables authentication for an OSPF area.</td>
</tr>
<tr>
<td>ip ospf authentication</td>
<td>Specifies authentication type for an interface.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

\[ 10^8 / \text{bandwidth} \]

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.

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor database-filter</td>
<td>Filters outgoing LSAs to an OSPF neighbor.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Specifies the interval (in seconds); the value must be the same for all nodes on the network.</td>
</tr>
</tbody>
</table>

**Defaults**

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

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ospf hello-interval</td>
<td>Specifies the interval between hello packets that the Cisco IOS software sends on the interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ospf interface</td>
<td>Displays OSPF-related interface information.</td>
</tr>
<tr>
<td>show ip ospf neighbor</td>
<td>Displays OSPF-neighbor information on a per-interface basis.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Specifies the interval (in seconds). The value must be the same for all nodes on a specific network.</td>
</tr>
</tbody>
</table>

**Defaults**

10 seconds (Ethernet)

30 seconds (nonbroadcast)

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip ospf dead-interval</strong></td>
<td>Sets the time period for which hello packets must not have been seen before neighbors declare the router down.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area authentication</td>
<td>Enables authentication for an OSPF area.</td>
</tr>
<tr>
<td>ip ospf authentication</td>
<td>Specifies authentication type for an interface.</td>
</tr>
<tr>
<td>service password-encryption</td>
<td>Encrypts a password.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(3)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```

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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>broadcast</code></td>
<td>Sets the network type to broadcast.</td>
</tr>
<tr>
<td><code>non-broadcast</code></td>
<td>Sets the network type to nonbroadcast multiaccess (NBMA).</td>
</tr>
<tr>
<td><code>point-to-multipoint</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>point-to-point</code></td>
<td>Sets the network type to point-to-point.</td>
</tr>
</tbody>
</table>

**Defaults**

Depends on the network type.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>10.3</td>
<td>The point-to-multipoint keyword was added.</td>
</tr>
<tr>
<td>11.3 AA</td>
<td>The non-broadcast keyword used with the point-to-multipoint keyword was added.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
interface serial 0
ip address 192.168.192.168.77.17 255.255.255.0
ip ospf network broadcast
encapsulation frame-relay
```

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

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>frame-relay map</code></td>
<td>Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.</td>
</tr>
<tr>
<td><code>neighbor (OSPF)</code></td>
<td>Configures OSPF routers interconnecting to nonbroadcast networks.</td>
</tr>
<tr>
<td><code>x25 map</code></td>
<td>Sets up the LAN protocols-to-remote host mapping.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ospf network</td>
<td>Configures the OSPF network type to a type other than the default for a given medium.</td>
</tr>
<tr>
<td>neighbor (OSPF)</td>
<td>Configures OSPF routers interconnecting to nonbroadcast networks.</td>
</tr>
</tbody>
</table>
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.

```plaintext
ip ospf retransmit-interval seconds

no ip ospf retransmit-interval
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Defaults**

5 seconds

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.</td>
</tr>
</tbody>
</table>

**Defaults**

Enabled

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced as &quot;ospf log-adjacency-changes&quot;.</td>
</tr>
<tr>
<td>12.1</td>
<td>The ospf keyword was omitted and the detail keyword was added.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.3 AA</td>
<td>The <code>cost</code> keyword was added.</td>
</tr>
</tbody>
</table>

**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.

**Note**
You cannot use the `neighbor (OSPF)` command to specify an Open Shortest Path First (OSPF) neighbor on non-broadcast networks within an OSPF Virtual Private Network (VPN) routing instance.

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-dlc 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ospf priority</td>
<td>Sets the router priority, which helps determine the designated router for this network.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address all out</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP address of the neighbor to which outgoing LSAs are blocked.</td>
</tr>
</tbody>
</table>

Defaults

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

Command Modes

Router configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Description</td>
</tr>
<tr>
<td>ip ospf database-filter all out</td>
</tr>
<tr>
<td>Filters outgoing LSAs to an OSPF interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address.</td>
</tr>
<tr>
<td>wildcard-mask</td>
<td>IP-address-type mask that includes “don’t care” bits.</td>
</tr>
<tr>
<td>area-id</td>
<td>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 <code>area-id</code> argument.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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.
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router ospf</td>
<td>Configures an OSPF routing process.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
routing-id 10.1.1.1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip ospf</td>
<td>Clears redistribution based on the OSPF routing process ID.</td>
</tr>
<tr>
<td>router ospf</td>
<td>Configures the OSPF routing process.</td>
</tr>
</tbody>
</table>
router ospf

To configure an Open Shortest Path First (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 [vrf vpn-name]

no router ospf process-id [vrf vpn-name]
```

**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.
- `vrf vpn-name` (Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with OSPF VRF processes.

**Defaults**

No OSPF routing process is defined.

**Command Modes**

Global configuration

**Command History**

```
Release Modification
10.0 This command was introduced.
12.0(7)T The `vrf` keyword and `vpn-name` arguments were added to identify a VPN.
12.0(9)ST The `vrf` keyword and `vpn-name` arguments were added.
```

**Usage Guidelines**

You can specify multiple OSPF routing processes in each router.

After you enter the `router ospf` command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

**Examples**

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

```
router ospf 109
```

This example shows a basic OSPF configuration using the `router ospf` command to configure OSPF VPN routing and forwarding (VRF) instance processes for the VRFs first, second, and third:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 12 vrf first
Router(config)# router ospf 13 vrf second
Router(config)# router ospf 14 vrf third
Router(config)# exit
```
The following example shows usage of the `maximum-paths` option:

Router> enable
Router# configure terminal
Router(config)# router ospf
Router(config-router)# maximum-paths?
Router(config)# 20
Router(config)# exit

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>network area</code></td>
<td>Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing process “ospf 201” with ID 192.42.110.200</td>
<td>Process ID and OSPF router ID.</td>
</tr>
<tr>
<td>Supports ...</td>
<td>Number of types of service supported (Type 0 only).</td>
</tr>
<tr>
<td>It is ...</td>
<td>Possible types are internal, area border, or autonomous system boundary.</td>
</tr>
<tr>
<td>Summary Link update interval</td>
<td>Specifies summary update interval in hours:minutes:seconds, and time until next update.</td>
</tr>
</tbody>
</table>
### Table 5  
*show ip ospf Field Descriptions (continued)*

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
Codes: i - Intra-area route, I - Inter-area route
i 192.168.97.53 [10] via 172.16.1.53, Serial0, ABR, Area 0.0.0.3, SPF 3
i 192.168.103.51 [10] via 192.168.96.51, Serial0, ABR, Area 0.0.0.3, SPF 3
I 192.168.103.52 [22] via 192.168.96.51, Serial0, ASBR, Area 0.0.0.3, SPF 3
I 192.168.103.52 [22] via 172.16.1.53, Serial0, ASBR, Area 0.0.0.3, SPF 3
```

Table 6 describes the significant fields shown in the display.

**Table 6  show ip ospf border-routers Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.97.53</td>
<td>Router ID of the destination.</td>
</tr>
<tr>
<td>[10]</td>
<td>Cost of using this route.</td>
</tr>
<tr>
<td>via 172.16.1.53</td>
<td>Next hop toward the destination.</td>
</tr>
<tr>
<td>Serial0</td>
<td>Interface type for the outgoing interface.</td>
</tr>
<tr>
<td>ABR</td>
<td>The router type of the destination; it is either an ABR or ASBR or both.</td>
</tr>
<tr>
<td>Area</td>
<td>The area ID of the area from which this route is learned.</td>
</tr>
<tr>
<td>SPF 3</td>
<td>The internal number of the shortest path first (SPF) calculation that installs this route.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>process-id</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>area-id</strong></td>
<td>(Optional) Area number associated with the OSPF address range defined in the network router configuration command used to define the particular area.</td>
</tr>
<tr>
<td><strong>adv-router</strong></td>
<td>(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).</td>
</tr>
<tr>
<td><strong>asbr-summary</strong></td>
<td>(Optional) Displays information only about the Autonomous System Boundary Router (ASBR) summary LSAs.</td>
</tr>
<tr>
<td><strong>link-state-id</strong></td>
<td>(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:</td>
</tr>
<tr>
<td><strong>database-summary</strong></td>
<td>(Optional) Displays how many of each type of LSA for each area there are in the database, and the total.</td>
</tr>
<tr>
<td><strong>external</strong></td>
<td>(Optional) Displays information only about the external LSAs.</td>
</tr>
<tr>
<td><strong>network</strong></td>
<td>(Optional) Displays information only about the network LSAs.</td>
</tr>
<tr>
<td><strong>nssa-external</strong></td>
<td>(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.</td>
</tr>
<tr>
<td><strong>opaque-area</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>opaque-as</strong></td>
<td>(Optional) Displays information about the opaque Type 11 LSAs. Type 11 denotes that the LSA is flooded throughout the autonomous system.</td>
</tr>
<tr>
<td><strong>opaque-link</strong></td>
<td>(Optional) Displays information about the opaque Type 9 LSAs. Type 9 denotes a link-local scope.</td>
</tr>
<tr>
<td><strong>router</strong></td>
<td>(Optional) Displays information only about the router LSAs.</td>
</tr>
<tr>
<td><strong>self-originate</strong></td>
<td>(Optional) Displays only self-originated LSAs (from the local router).</td>
</tr>
<tr>
<td><strong>summary</strong></td>
<td>(Optional) Displays information only about the summary LSAs.</td>
</tr>
</tbody>
</table>

### Command Modes

<table>
<thead>
<tr>
<th>Command</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ospf database</td>
<td>EXEC</td>
</tr>
</tbody>
</table>
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0</td>
<td>The <strong>database-summary</strong> keyword was added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The following keywords were added:</td>
</tr>
<tr>
<td></td>
<td>- <strong>self-originated</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>adv-router</strong></td>
</tr>
<tr>
<td>12.1</td>
<td>The following keywords were added:</td>
</tr>
<tr>
<td></td>
<td>- <strong>opaque-area</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>opaque-as</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>opaque-link</strong></td>
</tr>
</tbody>
</table>

### Examples

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

```plaintext
Router# show ip ospf database

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

Router Link States (Area 0)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
<th>Link count</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.8</td>
<td>192.168.1.8</td>
<td>1381</td>
<td>0x8000010D</td>
<td>0xEF60</td>
<td>2</td>
</tr>
<tr>
<td>192.168.1.11</td>
<td>192.168.1.11</td>
<td>1460</td>
<td>0x8000020E</td>
<td>0xEB3D</td>
<td>4</td>
</tr>
<tr>
<td>192.168.1.12</td>
<td>192.168.1.12</td>
<td>2027</td>
<td>0x80000090</td>
<td>0x875D</td>
<td>3</td>
</tr>
<tr>
<td>192.168.1.27</td>
<td>192.168.1.27</td>
<td>1323</td>
<td>0x800001D6</td>
<td>0x12CC</td>
<td>3</td>
</tr>
</tbody>
</table>

Net Link States (Area 0)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.27</td>
<td>192.168.1.27</td>
<td>1323</td>
<td>0x800005B</td>
<td>0xA8EE</td>
<td></td>
</tr>
<tr>
<td>172.17.1.11</td>
<td>192.168.1.11</td>
<td>1461</td>
<td>0x800005B</td>
<td>0x7AC</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
<th>Opaque ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0</td>
<td>192.168.1.11</td>
<td>1461</td>
<td>0x800002BC</td>
<td>0x8483</td>
<td>0</td>
</tr>
<tr>
<td>10.0.0.0</td>
<td>192.168.1.12</td>
<td>2027</td>
<td>0x80000080</td>
<td>0x8F58</td>
<td>0</td>
</tr>
<tr>
<td>10.0.0.0</td>
<td>192.168.1.27</td>
<td>1323</td>
<td>0x800001BC</td>
<td>0x919B</td>
<td>0</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>192.168.1.11</td>
<td>1461</td>
<td>0x8000005E</td>
<td>0x5B43</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 7 describes the significant fields shown in the display.

### Table 7  `show ip ospf database` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link ID</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>ADV Router</td>
<td>Advertising router ID.</td>
</tr>
<tr>
<td>Age</td>
<td>Link-state age.</td>
</tr>
<tr>
<td>Seq#</td>
<td>Link-state sequence number (detects old or duplicate LSAs).</td>
</tr>
<tr>
<td>Checksum</td>
<td>Fletcher checksum of the complete contents of the LSA.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router with id</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>Process ID</td>
<td>OSPF process ID.</td>
</tr>
<tr>
<td>LS age</td>
<td>Link-state age.</td>
</tr>
<tr>
<td>Options</td>
<td>Type of service options (Type 0 only).</td>
</tr>
<tr>
<td>LS Type</td>
<td>Link-state type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Link-state ID (ASBR).</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Advertising router ID.</td>
</tr>
<tr>
<td>LS Seq Number</td>
<td>Link-state sequence (detects old or duplicate LSAs).</td>
</tr>
<tr>
<td>Checksum</td>
<td>Link-state checksum (Fletcher checksum of the complete contents of the LSA).</td>
</tr>
<tr>
<td>Length</td>
<td>Length in bytes of the LSA.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Network mask implemented.</td>
</tr>
<tr>
<td>TOS</td>
<td>Type of service.</td>
</tr>
<tr>
<td>Metric</td>
<td>Link-state metric.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router with id</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>Autonomous system</td>
<td>OSPF autonomous system number (OSPF process ID).</td>
</tr>
<tr>
<td>LS age</td>
<td>Link-state age.</td>
</tr>
<tr>
<td>Options</td>
<td>Type of service options (Type 0 only).</td>
</tr>
<tr>
<td>LS Type</td>
<td>Link-state type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Link-state ID (external network number).</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Advertising router ID.</td>
</tr>
<tr>
<td>LS Seq Number</td>
<td>Link-state sequence number (detects old or duplicate LSAs).</td>
</tr>
<tr>
<td>Checksum</td>
<td>Checksum (Fletcher checksum of the complete contents of the LSA).</td>
</tr>
<tr>
<td>Length</td>
<td>Length in bytes of the LSA.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Network mask implemented.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>External type.</td>
</tr>
<tr>
<td>TOS</td>
<td>Type of service.</td>
</tr>
<tr>
<td>Metric</td>
<td>Link-state metric.</td>
</tr>
<tr>
<td>Forward Address</td>
<td>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.</td>
</tr>
<tr>
<td>External Route Tag</td>
<td>External route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.</td>
</tr>
</tbody>
</table>
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**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router with id</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>Process ID</td>
<td>OSPF process ID.</td>
</tr>
<tr>
<td>LS age</td>
<td>Link-state age.</td>
</tr>
<tr>
<td>Options</td>
<td>Type of service options (Type 0 only).</td>
</tr>
<tr>
<td>LS Type</td>
<td>Link-state type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Link-state ID.</td>
</tr>
<tr>
<td>Opaque Type</td>
<td>Opaque link-state type.</td>
</tr>
<tr>
<td>Opaque ID</td>
<td>Opaque ID number.</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Advertising router ID.</td>
</tr>
<tr>
<td>LS Seq Number</td>
<td>Link-state sequence (detects old or duplicate LSAs)</td>
</tr>
<tr>
<td>Checksum</td>
<td>Checksum (Fletcher checksum of the complete contents of the LSA).</td>
</tr>
</tbody>
</table>
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 11  `show ip ospf database opaque-area Field Descriptions (continued)`

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

Table 12  `show ip ospf database router Field Descriptions`

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router with id</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>Process ID</td>
<td>OSPF process ID.</td>
</tr>
<tr>
<td>LS age</td>
<td>Link-state age.</td>
</tr>
<tr>
<td>Options</td>
<td>Type of service options (Type 0 only).</td>
</tr>
</tbody>
</table>
### show ip ospf database router Field Descriptions (continued)

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

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.

### show ip ospf database summary Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router with id</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>Process ID</td>
<td>OSPF process ID.</td>
</tr>
<tr>
<td>LS age</td>
<td>Link-state age.</td>
</tr>
<tr>
<td>Options</td>
<td>Type of service options (Type 0 only).</td>
</tr>
<tr>
<td>LS Type</td>
<td>Link-state type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Link-state ID (summary network number).</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>The ID of the advertising router.</td>
</tr>
<tr>
<td>LS Seq Number</td>
<td>Link-state sequence (detects old or duplicate LSAs).</td>
</tr>
<tr>
<td>Checksum</td>
<td>Checksum (Fletcher checksum of the complete contents of the LSA).</td>
</tr>
<tr>
<td>Length</td>
<td>Length in bytes of the link-state advertisement.</td>
</tr>
</tbody>
</table>
### Table 13 show ip ospf database summary Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Mask</td>
<td>Network mask implemented.</td>
</tr>
<tr>
<td>TOS</td>
<td>Type of service.</td>
</tr>
<tr>
<td>Metric</td>
<td>Link-state metric.</td>
</tr>
</tbody>
</table>

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        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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>Area number.</td>
</tr>
<tr>
<td>Router</td>
<td>Number of router LSAs in that area.</td>
</tr>
<tr>
<td>Network</td>
<td>Number of network LSAs in that area.</td>
</tr>
<tr>
<td>Sum-Net</td>
<td>Number of summary LSAs in that area.</td>
</tr>
<tr>
<td>Sum-ASBR</td>
<td>Number of summary ASBR LSAs in that area.</td>
</tr>
<tr>
<td>Subtotal</td>
<td>Sum of Router, Network, Sum-Net, and Sum-ASBR for that area.</td>
</tr>
<tr>
<td>Delete</td>
<td>Number of LSAs that are marked “Deleted” in that area.</td>
</tr>
<tr>
<td>Maxage</td>
<td>Number of LSAs that are marked “Maxaged” in that area.</td>
</tr>
<tr>
<td>AS External</td>
<td>Number of external LSAs.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Type</th>
<th>LS ID</th>
<th>ADV RTR</th>
<th>Seq NO</th>
<th>Age</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>10.2.195.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0xFB61</td>
</tr>
<tr>
<td>5</td>
<td>10.2.192.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0x2938</td>
</tr>
<tr>
<td>5</td>
<td>10.2.194.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0x757</td>
</tr>
<tr>
<td>5</td>
<td>10.1.193.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0x1E42</td>
</tr>
<tr>
<td>5</td>
<td>10.2.193.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0x124D</td>
</tr>
<tr>
<td>5</td>
<td>10.1.194.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0x134C</td>
</tr>
</tbody>
</table>
```

Table 15 describes the significant fields shown in the display.

**Table 15 show ip ospf flood-list Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Ethernet1</td>
<td>Interface for which information is displayed.</td>
</tr>
<tr>
<td>Queue length</td>
<td>Number of LSAs waiting to be flooded.</td>
</tr>
<tr>
<td>Link state retransmission due in</td>
<td>Length of time before next link-state transmission.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of LSA.</td>
</tr>
<tr>
<td>LS ID</td>
<td>Link-state ID of the LSA.</td>
</tr>
<tr>
<td>ADV RTR</td>
<td>IP address of advertising router.</td>
</tr>
<tr>
<td>Seq NO</td>
<td>Sequence number of LSA.</td>
</tr>
</tbody>
</table>
### Table 15  show ip ospf flood-list Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Age of LSA (in seconds).</td>
</tr>
<tr>
<td>Checksum</td>
<td>Checksum of LSA.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Interface number.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>Status of physical link and operational status of protocol.</td>
</tr>
<tr>
<td>Internet Address</td>
<td>Interface IP address, subnet mask, and area address.</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous system number (OSPF process ID), router ID, network type, link-state cost.</td>
</tr>
<tr>
<td>Transmit Delay</td>
<td>Transmit delay, interface state, and router priority.</td>
</tr>
<tr>
<td>Designated Router</td>
<td>Designated router ID and respective interface IP address.</td>
</tr>
<tr>
<td>Backup Designated router</td>
<td>Backup designated router ID and respective interface IP address.</td>
</tr>
<tr>
<td>Timer intervals configured</td>
<td>Configuration of timer intervals.</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>Number of seconds until next hello packet is sent out this interface.</td>
</tr>
<tr>
<td>Neighbor Count</td>
<td>Count of network neighbors and list of adjacent neighbors.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Neighbor router ID.</td>
</tr>
<tr>
<td>interface address</td>
<td>IP address of the interface.</td>
</tr>
<tr>
<td>In the area</td>
<td>Area and interface through which the OSPF neighbor is known.</td>
</tr>
<tr>
<td>Neighbor priority</td>
<td>Router priority of the neighbor, neighbor state.</td>
</tr>
<tr>
<td>State</td>
<td>OSPF state.</td>
</tr>
<tr>
<td>state changes</td>
<td>Number of state changes since the neighbor was created. This value can be</td>
</tr>
<tr>
<td></td>
<td>reset using the <code>clear ip ospf counters neighbor</code> command.</td>
</tr>
<tr>
<td>DR is</td>
<td>Router ID of the designated router for the interface.</td>
</tr>
<tr>
<td>BDR is</td>
<td>Router ID of the backup designated router for the interface.</td>
</tr>
<tr>
<td>Options</td>
<td>Hello packet options field contents. (E-bit only. Possible values are 0 and</td>
</tr>
<tr>
<td></td>
<td>2; 2 indicates area is not a stub; 0 indicates area is a stub.)</td>
</tr>
<tr>
<td>Dead timer</td>
<td>Expected time before Cisco IOS software will declare the neighbor dead.</td>
</tr>
</tbody>
</table>
```
### Table 17  show ip ospf neighbor detail Field Descriptions (continued)

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Type</th>
<th>LS ID</th>
<th>ADV RTR</th>
<th>Seq NO</th>
<th>Age</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.1.12</td>
<td>192.168.1.12</td>
<td>0x8000020D</td>
<td>8</td>
<td>0x6572</td>
</tr>
</tbody>
</table>
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 Serial10 address 172.16.1.11
Link state retransmission due in 3764 msec, Queue length 2

<table>
<thead>
<tr>
<th>Type</th>
<th>LS ID</th>
<th>ADV RTR</th>
<th>Seq NO</th>
<th>Age</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.1.12</td>
<td>192.168.1.12</td>
<td>0x80000210</td>
<td>0</td>
<td>0xB196</td>
</tr>
</tbody>
</table>
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Routes learned from other routing protocols can 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
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>area range</td>
<td>Consolidates and summarizes routes at an area boundary.</td>
</tr>
<tr>
<td></td>
<td><strong>ip ospf authentication-key</strong></td>
<td>Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.</td>
</tr>
<tr>
<td></td>
<td><strong>ip ospf message-digest-key</strong></td>
<td>Enables OSPF MD5 authentication.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 AA</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>spf-delay</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>spf-holdtime</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
timers spf
EIGRP Commands

Use the commands in this chapter to configure and monitor Enhanced Interior Gateway Routing Protocol (EIGRP). For EIGRP configuration information and examples, refer to the “Configuring IP EIGRP” chapter of the Cisco IOS IP Configuration Guide.
auto-summary (EIGRP)

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.

Enhanced Interior Gateway Routing Protocol (EIGRP) 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 EIGRP process 1:

```
router eigrp 1
no auto-summary
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip summary-address eigrp</td>
<td>Configures a summary aggregate address for a specified interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip eigrp</td>
<td>Displays information about interfaces configured for EIGRP.</td>
</tr>
<tr>
<td>interfaces</td>
<td></td>
</tr>
</tbody>
</table>
default-information

To control the candidate default routing information between IGRP or Enhanced Interior Gateway Routing Protocol (EIGRP) processes, use the `default-information` command in router configuration mode. To suppress IGRP or EIGRP 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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>Allows IGRP or EIGRP exterior or default routes to be received by an IGRP process.</td>
</tr>
<tr>
<td>out</td>
<td>Allows IGRP or EIGRP exterior routes to be advertised in updates.</td>
</tr>
<tr>
<td>access-list-number</td>
<td>Number or name of an access list. It can be a number in the range from 1 to 99 or an access list name.</td>
</tr>
<tr>
<td>access-list-name</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-number</code> and <code>access-list-name</code> arguments were added.</td>
</tr>
</tbody>
</table>

**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 EIGRP.

**Examples**

The following example allows IGRP exterior or default routes to be received by the IGRP process in autonomous system 1:

```
router igrp 1
   default-information in
```

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

```
router eigrp 1
   default-information in
```
default-metric (EIGRP)

To set metrics for IGRP or Enhanced Interior Gateway Routing Protocol (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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth</td>
<td>Minimum bandwidth of the route in kilobits per second. It can be from 1 to 4294967295.</td>
</tr>
<tr>
<td>delay</td>
<td>Route delay in tens of microseconds. It can be 1 or any positive number that is a multiple of 39.1 nanoseconds.</td>
</tr>
<tr>
<td>reliability</td>
<td>Likelihood of successful packet transmission expressed as a number between 0 and 255. The value 255 means 100 percent reliability; 0 means no reliability.</td>
</tr>
<tr>
<td>loading</td>
<td>Effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).</td>
</tr>
<tr>
<td>mtu</td>
<td>Minimum maximum transmission unit (MTU) size of the route in bytes. It can be from 1 to 65535.</td>
</tr>
</tbody>
</table>

### Defaults

Only connected routes can be redistributed without a default metric. The metric of redistributed connected routes is set to 0.

### Command Modes

Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 care when changing these values. Keeping the same metrics is supported only when redistributing from IGRP, EIGRP, or static routes.
**Note**

When enabled, the `default-metric` command applies a metric value of 0 to redistributed connected routes. The `default-metric` command does not override metric values that are applied with the `redistribute` command.

**Examples**

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

```
router eigrp 1
network 172.16.0.0
redistribute rip
default-metric 1000 100 250 100 1500
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
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 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**: 10.0
- **Modification**: 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**

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route</td>
<td>1</td>
</tr>
<tr>
<td>EIGRP summary route</td>
<td>5</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
</tbody>
</table>
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 EIGRP routing in autonomous system number 1. The `network` router configuration commands specify EIGRP 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 1
Router(config-router)# network 192.168.7.0
Router(config-router)# network 172.16.0.0
Router(config-router)# 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.

**Table 19  Default Administrative Distances (continued)**

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal EIGRP</td>
<td>90</td>
</tr>
<tr>
<td>IGRP</td>
<td>100</td>
</tr>
<tr>
<td>Open Shortest Path First (OSPF)</td>
<td>110</td>
</tr>
<tr>
<td>Intermediate System-to-Intermediate System (IS-IS)</td>
<td>115</td>
</tr>
<tr>
<td>Routing Information Protocol (RIP)</td>
<td>120</td>
</tr>
<tr>
<td>Exterior Gateway Protocol (EGP)</td>
<td>140</td>
</tr>
<tr>
<td>EIGRP external route</td>
<td>170</td>
</tr>
<tr>
<td>Internal Border Gateway Protocol (BGP)</td>
<td>200</td>
</tr>
<tr>
<td>Unknown</td>
<td>255</td>
</tr>
</tbody>
</table>

To display the default administrative distance for a specified routing process, use the `show ip protocols` EXEC command.
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.

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-number</code>, <code>interface-type</code>, and <code>interface-number</code> arguments were added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>prefix-list-name</code> argument was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>
This command is not supported in Intermediate System-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 172.18.0.0:

```plaintext
access-list 1 permit 0.0.0.0
access-list 1 permit 172.18.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router bgp 5000
   network 172.18.0.0
   distribute-list 1 in
```

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

```plaintext
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
router rip
   network 172.18.0.0
   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:

```plaintext
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
ip prefix-list allowlist seq 5 permit 192.168.1.1/32
router rip
   network 172.18.0.0
   distribute-list prefix max24 gateway allowlist in
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>distribute-list out (RIP, IGRP, EIGRP)</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-number</code> argument was added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>prefix-list-name</code> argument was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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.
Specifying 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 172.18.0.0) to be advertised by a RIP routing process:

```plaintext
access-list 1 permit 172.18.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router rip
    network 172.18.0.0
    distribute-list 1 out
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>distribute-list in (RIP, IGRP, EIGRP)</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
</tbody>
</table>
**eigrp log-neighbor-changes**

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (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**

Adjacency changes are logged.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems. Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the `no` form of this command.

**Examples**

The following configuration disables logging of neighbor changes for EIGRP process 1:

```
router eigrp 1
no eigrp log-neighbor-changes
```

The following configuration enables logging of neighbor changes for EIGRP process 1:

```
router eigrp 1
eigrp log-neighbor-changes
```
**eigrp log-neighbor-warnings**

To enable the logging of Enhanced Interior Gateway Routing Protocol (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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 1 and repeat the warning messages in 5-minute (300 seconds) intervals:

```
router eigrp 1
eigrp log-neighbor-warnings 300
```
**eigrp router-id**

To set the router ID used by Enhanced Interior Gateway Routing Protocol (EIGRP) when communicating with its neighbors, use the `eigrp router-id` command in router configuration mode. To remove the configured router ID, use the `no` form of this command.

```
eigrp router-id ip-address
no eigrp router-id ip-address
```

**Syntax Description**

```
ip-address  Router ID in dotted decimal notation.
```

**Defaults**

EIGRP automatically selects an IP address to use as the router ID when an EIGRP process is started. The highest local IP address is selected and loopback interfaces are preferred. The router ID is not changed unless the EIGRP process is removed with the `no router eigrp` command or if the router ID is manually configured with the `eigrp router-id` command.

**Command Modes**

- Address family configuration
- Router configuration

**Command History**

```
Release  Modification
12.1     This command was introduced.
```

**Usage Guidelines**

The router ID is used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. The router ID can be configured with any IP address with two exceptions; 0.0.0.0 and 255.255.255.255 are not legal values and cannot be entered. A unique value should be configured for each router.

**Examples**

The following example configures 172.16.1.3 as a fixed router ID:

```
router eigrp 1
  eigrp router-id 172.16.1.3
```
eigrp stub

To configure a router as a stub using Enhanced Interior Gateway Routing Protocol (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 | redistributed]

no eigrp stub [receive-only | connected | static | summary | redistributed]
```

**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.
- **redistributed** (Optional) Advertises redistributed routes from other protocols and autonomous systems.

**Defaults**

Stub routing is not enabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(15)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(15)S.</td>
</tr>
<tr>
<td>12.2</td>
<td>Keyword <code>redistributed</code> was added.</td>
</tr>
</tbody>
</table>

**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 four other optional keywords (`connected`, `static`, `summary`, and `redistributed`) can be used in any combination but cannot be used with the `receive-only` keyword.

If any of these four keywords is used with the `eigrp stub` command, only the route types specified by the particular keyword(s) will be sent. Route types specified by the non-used keyword(s) will not be sent.

The `connected` keyword permits 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 permits 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 permits 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.

The **redistributed** keyword permits the EIGRP Stub Routing feature to send other routing protocols and autonomous systems. Without the configuration of this option, EIGRP will not advertise redistributed routes.

[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:

```plaintext
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):

```plaintext
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):

```plaintext
router eigrp 1
network 10.0.0.0 eigrp
eigrp stub receive-only
```

In the following example, the `eigrp stub` command is issued with the `redistributed` keyword to configure the router to advertise other protocols and autonomous systems:

```plaintext
router eigrp 1
network 10.0.0.0 eigrp
eigrp stub redistributed
```
ip authentication key-chain eigrp

To enable authentication of Enhanced Interior Gateway Routing Protocol (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.

```plaintext
ip authentication key-chain eigrp as-number key-chain
no ip authentication key-chain eigrp as-number key-chain
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as-number</td>
<td>Autonomous system number to which the authentication applies.</td>
</tr>
<tr>
<td>key-chain</td>
<td>Name of the authentication key chain.</td>
</tr>
</tbody>
</table>

### Defaults

No authentication is provided for EIGRP packets.

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example applies authentication to autonomous system 2 and identifies a key chain named SPORTS:

```plaintext
ip authentication key-chain eigrp 2 SPORTS
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime</td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td>ip authentication mode eigrp</td>
<td>Specifies the type of authentication used in EIGRP packets.</td>
</tr>
<tr>
<td>key</td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td>key chain</td>
<td>Enables authentication of routing protocols.</td>
</tr>
<tr>
<td>key-string (authentication)</td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td>send-lifetime</td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
</tbody>
</table>
**ip authentication mode eigrp**

To specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 1:

```
ip authentication mode eigrp 1 md5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime</td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td>ip authentication key-chain eigrp</td>
<td>Enables authentication of EIGRP packets.</td>
</tr>
<tr>
<td>key</td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td>key chain</td>
<td>Enables authentication of routing protocols.</td>
</tr>
<tr>
<td>key-string (authentication)</td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td>send-lifetime</td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
</tbody>
</table>
ip bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the `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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 1:

```
interface serial 0
bandwidth 56
ip bandwidth-percent eigrp 1 75
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth (interface)</td>
<td>Sets a bandwidth value for an interface.</td>
</tr>
</tbody>
</table>
ip hello-interval eigrp

To configure the hello interval for the Enhanced Interior Gateway Routing Protocol (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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as-number</td>
<td>Autonomous system number.</td>
</tr>
<tr>
<td>seconds</td>
<td>Hello interval (in seconds).</td>
</tr>
</tbody>
</table>

**Defaults**

- For low-speed, nonbroadcast multiaccess (NBMA) networks: 60 seconds
- For all other networks: 5 seconds

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 EIGRP, 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 1 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth (interface)</td>
<td>Sets a bandwidth value for an interface.</td>
</tr>
<tr>
<td>ip hold-time eigrp</td>
<td>Configures the hold time for a particular EIGRP routing process designated by the autonomous system number.</td>
</tr>
</tbody>
</table>
ip hold-time eigrp

To configure the hold time for a particular Enhanced Interior Gateway Routing Protocol (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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>as-number</code></td>
<td>Autonomous system number.</td>
</tr>
<tr>
<td><code>seconds</code></td>
<td>Hold time (in seconds).</td>
</tr>
</tbody>
</table>

**Defaults**

For low-speed, nonbroadcast multiaccess (NBMA) networks: 180 seconds

For all other networks: 15 seconds

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 1 40
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bandwidth</code></td>
<td>Sets a bandwidth value for an interface.</td>
</tr>
<tr>
<td><code>ip hello-interval eigrp</code></td>
<td>Configures the hello interval for the EIGRP routing process designated by an autonomous system number.</td>
</tr>
</tbody>
</table>
ip split-horizon eigrp

To enable Enhanced Interior Gateway Routing Protocol (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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip split-horizon (IGRP)</td>
<td>Enables the split horizon mechanism.</td>
</tr>
<tr>
<td>neighbor (IGRP)</td>
<td>Defines a neighboring router with which to exchange routing information.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>The <code>admin-distance</code> argument was added.</td>
</tr>
</tbody>
</table>

**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 1 192.168.0.0 255.255.0.0 95
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-summary (EIGRP)</td>
<td>Restores the default behavior of automatic summarization of subnet routes into network-level routes.</td>
</tr>
</tbody>
</table>
**metric weights (EIGRP)**

To allow the tuning of the IGRP or Enhanced Interior Gateway Routing Protocol (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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tos</td>
<td>Type of service must always be zero.</td>
</tr>
<tr>
<td>k1 k2 k3 k4 k5</td>
<td>Constants that convert an IGRP or EIGRP metric vector into a scalar quantity.</td>
</tr>
</tbody>
</table>

**Defaults**

```
tos: 0
k1: 1
k2: 0
k3: 1
k4: 0
k5: 0
```

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 $2.56 \times 10^{12}$. 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>
<thead>
<tr>
<th>Media Type</th>
<th>Delay</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satellite</td>
<td>5120 (2 seconds)</td>
<td>5120 (500 megabits)</td>
</tr>
<tr>
<td>Ethernet</td>
<td>25600 (1 milliseconds [ms])</td>
<td>256000 (10 megabits)</td>
</tr>
<tr>
<td>1.544 Mbps</td>
<td>512000 (20,000 ms)</td>
<td>1,657,856 bits</td>
</tr>
<tr>
<td>64 kbps</td>
<td>512000 (20,000 ms)</td>
<td>40,000,000 bits</td>
</tr>
<tr>
<td>56 kbps</td>
<td>512000 (20,000 ms)</td>
<td>45,714,176 bits</td>
</tr>
<tr>
<td>10 kbps</td>
<td>512000 (20,000 ms)</td>
<td>256,000,000 bits</td>
</tr>
<tr>
<td>1 kbps</td>
<td>512000 (20,000 ms)</td>
<td>2,560,000,000 bits</td>
</tr>
</tbody>
</table>

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:

```bash
router igrp 1
network 192.168.0.0
metric weights 0 2 0 2 0 0
```

### Related Commands

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

To define a neighboring router with which to exchange routing information on a router that is running Enhanced Interior Gateway Routing Protocol (EIGRP), use the `neighbor` command in router configuration mode. To remove an entry, use the `no` form of this command.

```
neighbor ip-address interface-type interface-number
no neighbor ip-address interface-type interface-number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of a peer router with which routing information will be exchanged.</td>
</tr>
<tr>
<td><code>interface-type</code></td>
<td>Interface through which peering is established.</td>
</tr>
<tr>
<td><code>interface-number</code></td>
<td>Number of the interface or subinterface.</td>
</tr>
</tbody>
</table>

**Command Default**

No neighboring routers are defined.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Multiple neighbor statements can be used to establish peering sessions with specific EIGRP neighbors. The interface through which EIGRP will exchange routing updates must be specified in the neighbor statement. The interfaces through which two EIGRP neighbors exchange routing updates must be configured with IP addresses from the same network.

**Note**

Configuring the `passive-interface` command suppresses all incoming and outgoing routing updates and hello messages. EIGRP neighbor adjacencies cannot be established or maintained over an interface that is configured as passive.

**Examples**

The following example configures EIGRP peering sessions with the 192.168.1.1 and 192.168.2.2 neighbors:

```
router eigrp 1
network 192.168.0.0
neighbor 192.168.1.1 Ethernet 0/0
neighbor 192.168.2.2 Ethernet 1/1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive-interface</td>
<td>Disables sending routing updates on an interface.</td>
</tr>
</tbody>
</table>
network (EIGRP)

To specify a list of networks for the Enhanced Interior Gateway Routing Protocol (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**

- **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 EIGRP and assigns autonomous system 1. The `network` commands indicate the networks directly connected to the router.

```
   router eigrp 1
   network 172.16.0.0
   network 192.168.7.0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>router eigrp</code></td>
<td>Configures the EIGRP routing process.</td>
</tr>
<tr>
<td><code>router igrp</code></td>
<td>Configures the IGRP routing process.</td>
</tr>
</tbody>
</table>
offset-list (EIGRP)

To add an offset to incoming and outgoing metrics to routes learned via Enhanced Interior Gateway Routing Protocol (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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-number</td>
<td>Standard access list number or name to be applied. Access list number 0 indicates all access lists. If the <code>offset</code> value is 0, no action is taken. For IGRP, the offset is added to the delay component only.</td>
</tr>
<tr>
<td>access-list-name</td>
<td></td>
</tr>
<tr>
<td>in</td>
<td>Applies the access list to incoming metrics.</td>
</tr>
<tr>
<td>out</td>
<td>Applies the access list to outgoing metrics.</td>
</tr>
<tr>
<td>offset</td>
<td>Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.</td>
</tr>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type to which the offset list is applied.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Interface number to which the offset list is applied.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>10.3</td>
<td>The <code>interface-type</code> and <code>interface-number</code> arguments were added.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-name</code> argument was added.</td>
</tr>
</tbody>
</table>

**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 Interior Gateway Routing Protocol (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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example configures an EIGRP routing process and assigns process number 1:

```
routerv eigrp 1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network (EIGRP)</td>
<td>Specifies a list of networks for the EIGRP routing process.</td>
</tr>
</tbody>
</table>
set metric (EIGRP)

To set the metric value for Enhanced Interior Gateway Routing Protocol (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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bandwidth</code></td>
<td>Metric value or EIGRP bandwidth of the route in kbps. It can be in the range 0 to 4294967295.</td>
</tr>
<tr>
<td><code>delay</code></td>
<td>Route delay (in tens of microseconds). It can be in the range from 0 to 4294967295.</td>
</tr>
<tr>
<td><code>reliability</code></td>
<td>Likelihood of successful packet transmission expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.</td>
</tr>
<tr>
<td><code>loading</code></td>
<td>Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).</td>
</tr>
<tr>
<td><code>mtu</code></td>
<td>Minimum maximum transmission unit (MTU) size of the route, in bytes. It can be in the range from 0 to 4294967295.</td>
</tr>
</tbody>
</table>

### Defaults

No metric will be set in the route map.

### Command Modes

Route-map configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 Interior Gateway Routing Protocol (EIGRP), use the `show ip eigrp interfaces` command in EXEC mode.

```
show ip eigrp interfaces [interface-type interface-number] [as-number]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Interface number.</td>
</tr>
<tr>
<td>as-number</td>
<td>(Optional) Autonomous system number.</td>
</tr>
</tbody>
</table>

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 1

Interface Peers Xmit Queue Mean Pacing Time Multicast Flow Timer Routes
Di0 0/0 11/434 0 0
Et0 1 0/0 10 1/63 0 0
SE0:1.16 1 0/0 0/10 0 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface over which EIGRP is configured.</td>
</tr>
<tr>
<td>Peers</td>
<td>Number of directly connected EIGRP neighbors.</td>
</tr>
</tbody>
</table>
### Table 21  show ip eigrp interfaces Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xmit Queue Un/Reliable</td>
<td>Number of packets remaining in the Unreliable and Reliable transmit queues.</td>
</tr>
<tr>
<td>Mean SRTT</td>
<td>Mean smooth round-trip time (SRTT) interval (in milliseconds).</td>
</tr>
<tr>
<td>Pacing Time Un/Reliable</td>
<td>Pacing time used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets).</td>
</tr>
<tr>
<td>Multicast Flow Timer</td>
<td>Maximum number of seconds in which the router will send multicast EIGRP packets.</td>
</tr>
<tr>
<td>Pending Routes</td>
<td>Number of routes in the packets in the transmit queue waiting to be sent.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip eigrp neighbors</td>
<td>Displays the neighbors discovered by EIGRP.</td>
</tr>
</tbody>
</table>
**show ip eigrp neighbors**

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>The <code>static</code> keyword was added.</td>
</tr>
</tbody>
</table>

**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 (secs) Uptime (h:m:s) Q  Seq  SRTT (ms)  RTO (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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process 77</td>
<td>Autonomous system number specified in the <code>router</code> configuration command.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the EIGRP peer.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the router is receiving hello packets from the peer.</td>
</tr>
<tr>
<td>Holdtime</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 22  show ip eigrp neighbors Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime</td>
<td>Elapsed time (in hours:minutes:seconds) since the local router first heard from this neighbor.</td>
</tr>
<tr>
<td>Q Count</td>
<td>Number of EIGRP packets (update, query, and reply) that the software is waiting to send.</td>
</tr>
<tr>
<td>Seq Num</td>
<td>Sequence number of the last update, query, or reply packet that was received from this neighbor.</td>
</tr>
<tr>
<td>SRTT</td>
<td>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.</td>
</tr>
<tr>
<td>RTO</td>
<td>Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.</td>
</tr>
</tbody>
</table>
show ip eigrp topology

To display entries in the Enhanced Interior Gateway Routing Protocol (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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>as-number</strong></td>
<td>(Optional) Autonomous system number.</td>
</tr>
<tr>
<td><strong>ip-address</strong></td>
<td>(Optional) IP address. When specified with a mask, a detailed description of the entry is provided.</td>
</tr>
<tr>
<td><strong>mask</strong></td>
<td>(Optional) Subnet mask.</td>
</tr>
<tr>
<td><strong>active</strong></td>
<td>(Optional) Displays only active entries in the EIGRP topology table.</td>
</tr>
<tr>
<td><strong>all-links</strong></td>
<td>(Optional) Displays all entries in the EIGRP topology table.</td>
</tr>
<tr>
<td><strong>pending</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>summary</strong></td>
<td>(Optional) Displays a summary of the EIGRP topology table.</td>
</tr>
<tr>
<td><strong>zero-successors</strong></td>
<td>(Optional) Displays available routes in the EIGRP topology table.</td>
</tr>
</tbody>
</table>

### Command Modes

- EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codes</td>
<td>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.</td>
</tr>
<tr>
<td>P – Passive</td>
<td>No EIGRP computations are being performed for this destination.</td>
</tr>
<tr>
<td>A – Active</td>
<td>EIGRP computations are being performed for this destination.</td>
</tr>
<tr>
<td>U – Update</td>
<td>Indicates that an update packet was sent to this destination.</td>
</tr>
<tr>
<td>Q – Query</td>
<td>Indicates that a query packet was sent to this destination.</td>
</tr>
<tr>
<td>R – Reply</td>
<td>Indicates that a reply packet was sent to this destination.</td>
</tr>
<tr>
<td>r – Reply status</td>
<td>Flag that is set after the software has sent a query and is waiting for a reply.</td>
</tr>
<tr>
<td>172.16.90.0</td>
<td>Destination IP network number.</td>
</tr>
<tr>
<td>255.255.255.0</td>
<td>Destination subnet mask.</td>
</tr>
<tr>
<td>successors</td>
<td>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.</td>
</tr>
<tr>
<td>FD</td>
<td>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.</td>
</tr>
<tr>
<td>replies</td>
<td>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.</td>
</tr>
<tr>
<td>state</td>
<td>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.</td>
</tr>
<tr>
<td>via</td>
<td>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.</td>
</tr>
<tr>
<td>(46251776/46226176)</td>
<td>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.</td>
</tr>
<tr>
<td>Ethernet0</td>
<td>Interface from which this information was learned.</td>
</tr>
<tr>
<td>Serial0</td>
<td>Interface from which this information was learned.</td>
</tr>
</tbody>
</table>
show ip eigrp traffic

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets sent and received, use the `show ip eigrp traffic` command in EXEC mode.

```
show ip eigrp traffic [as-number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>as-number</code></td>
<td>(Optional) Autonomous system number.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process 77</td>
<td>Autonomous system number specified in the <code>ip router</code> command.</td>
</tr>
<tr>
<td>Hellos sent/received</td>
<td>Number of hello packets sent and received.</td>
</tr>
<tr>
<td>Updates sent/received</td>
<td>Number of update packets sent and received.</td>
</tr>
<tr>
<td>Queries sent/received</td>
<td>Number of query packets sent and received.</td>
</tr>
<tr>
<td>Replies sent/received</td>
<td>Number of reply packets sent and received.</td>
</tr>
<tr>
<td>Acks sent/received</td>
<td>Number of acknowledgment packets sent and received.</td>
</tr>
</tbody>
</table>
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 1 to 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 eigrp 1
    timers active-time 200
```

In the following example, the routing wait time is indefinite on the specified route:

```
router eigrp 1
    timers active-time disabled
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip eigrp topology</td>
<td>Displays the EIGRP topology table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 1
  traffic-share balanced
  variance 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>variance (EIGRP)</td>
<td>Controls load balancing in an EIGRP and IGRP internetwork.</td>
</tr>
</tbody>
</table>
variance (EIGRP)

To control load balancing in an Enhanced Interior Gateway Routing Protocol (EIGRP) 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

1. The local best metric must be greater than the metric learned from the next router.
2. 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 eigrp 1
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>password</code></td>
<td>Password you assign.</td>
</tr>
</tbody>
</table>

**Defaults**

No area password is defined, and area password authentication is disabled.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-password</td>
<td>Configures the IS-IS routing domain authentication password.</td>
</tr>
<tr>
<td>isis password</td>
<td>Configures the authentication password for an interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
<tr>
<td>show isis database</td>
<td>Displays the IS-IS link-state database.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>password</strong></td>
<td>Password you assign.</td>
</tr>
</tbody>
</table>

**Defaults**

No password is specified and no authentication is enabled for exchange of Level 2 routing information.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-password</td>
<td>Configures the IS-IS area authentication password.</td>
</tr>
<tr>
<td>isis password</td>
<td>Configures the authentication password for an interface.</td>
</tr>
</tbody>
</table>
**hello padding**

To reenable IS-IS hello padding at the router level, enter the `hello padding` command in router configuration mode. To disable IS-IS hello padding, use the `no` form of this command.

```
hello padding
no hello padding
```

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

**Defaults**
IS-IS hello padding is enabled.

**Command Modes**
Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(5)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(5)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Intermediate System-to-Intermediate System (IS-IS) hellos are padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

You can disable hello padding in order to avoid wasting network bandwidth in case the MTU of both interfaces is the same or, in case of translational bridging. While hello padding is disabled, Cisco routers still send the first five IS-IS hellos padded to the full MTU size, in order to maintain the benefits of discovering MTU mismatches.

To disable hello padding for all interfaces on a router for the IS-IS routing process, enter the `no hello padding` command in router configuration mode. To selectively disable hello padding for a specific interface, enter the `no isis hello padding` command in interface configuration mode.

**Examples**
In the following example the `no hello padding` command is used to turn off hello padding at the router level:

```
Router(config)# router isis
Router(config-router)# no hello padding
Router(config-router)# end
```

The `show clns interfaces` command is entered to show that hello padding has been turned off at router level:

```
Router# show clns interface e0/0

Ethernet0/0 is up, line protocol is up
  checksums enabled, MTU 1497, Encapsulation SAP
```
Integrated IS-IS Commands

**hello padding**

ERPDUs enabled, min. interval 10 msec.
CLNS fast switching enabled
CLNS SSE switching disabled
DEC compatibility mode OFF for this interface
Next ESH/ISH in 4 seconds
Routing Protocol: IS-IS
  Circuit Type: level-1-2
  Interface number 0x0, local circuit ID 0x1
  Level-1 Metric: 10, Priority: 64, Circuit ID: Router_B.01
  Level-1 IPv6 Metric: 10
  Number of active level-1 adjacencies: 1
  Level-2 Metric: 10, Priority: 64, Circuit ID: Router_B.01
  Level-2 IPv6 Metric: 10
  Number of active level-2 adjacencies: 1
  Next IS-IS LAN Level-1 Hello in 6 seconds
! No hello padding
  Next IS-IS LAN Level-2 Hello in 2 seconds
! No hello padding

When the **debug isis adj packets** command is entered, the output will show the IS-IS hello protocol data unit (PDU) length when a hello packet has been sent to or received from an IS-IS adjacency. In the following example the IS-IS hello PDU length is 1497:

Router# debug isis adj packets e0/0

IS-IS Adjacency related packets debugging is on
Router_A#
  *Oct 11 18:04:17.455: ISIS-Adj: Sending L1 LAN IIH on Ethernet0/0, length 55
  *Oct 11 18:04:19.075: ISIS-Adj: Rec L2 IIH from aabb.cc00.6600 (Ethernet0/0), cir type L1L2, cir id 0000.0000.000B.01, length 1497

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>isis hello padding</strong></td>
<td>Reenables IS-IS hello padding at the interface level.</td>
</tr>
<tr>
<td></td>
<td><strong>debug isis adj packets</strong></td>
<td>Displays information on all adjacency-related activity such as hello packets sent and received and IS-IS adjacencies going up and down.</td>
</tr>
<tr>
<td></td>
<td><strong>show clns interface</strong></td>
<td>Lists the CLNS-specific information about each interface.</td>
</tr>
</tbody>
</table>
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 |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
<td></td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>Multiarea functionality was added, changing the way the tag argument (now area-tag) is used.</td>
<td></td>
</tr>
</tbody>
</table>

| 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:

```plaintext
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:

```plaintext
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
    !
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 49.2222.0000.0000.0000.0005.00
    !
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is-type</td>
<td>Configures the routing level for an IS-IS routing process.</td>
</tr>
<tr>
<td>net</td>
<td>Configures an IS-IS NET for a CLNS routing process.</td>
</tr>
<tr>
<td>router isis</td>
<td>Enables the IS-IS routing protocol.</td>
</tr>
</tbody>
</table>
**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 1 and Level 2, use the `no` form of this command.

```
isis circuit-type [level-1 | level-1-2 | level-2-only]

no isis circuit-type
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>(Optional) Configures a router for Level 1 adjacency only.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>(Optional) Configures a router for Level 1 and Level 2 adjacency.</td>
</tr>
<tr>
<td>level-2-only</td>
<td>(Optional) Configures a router for Level 2 adjacency only.</td>
</tr>
</tbody>
</table>

**Defaults**

A Level 1 and Level 2 adjacency is established.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show clns es-neighbors</td>
<td>Lists the ES neighbors that this router knows.</td>
</tr>
<tr>
<td>show clns is-neighbors</td>
<td>Displays IS-IS related information for IS-IS router adjacencies.</td>
</tr>
<tr>
<td>show clns neighbors</td>
<td>Displays both ES and IS neighbors.</td>
</tr>
<tr>
<td>show clns protocol</td>
<td>Lists the protocol-specific information for each ISO IGRP routing process in the router.</td>
</tr>
<tr>
<td>show clns traffic</td>
<td>Lists the CLNS packets this router has seen.</td>
</tr>
<tr>
<td>show isis database</td>
<td>Displays the IS-IS link-state database.</td>
</tr>
<tr>
<td>show isis routes</td>
<td>Displays the IS-IS Level 1 forwarding table for IS-IS learned routes.</td>
</tr>
<tr>
<td>show isis spf-log</td>
<td>Displays how often and why the router has run a full SPF calculation.</td>
</tr>
<tr>
<td>show isis topology</td>
<td>Displays a list of all connected routers in all areas.</td>
</tr>
</tbody>
</table>
isis hello padding

To reenable IS-IS hello padding at the interface level, enter the `isis hello padding` command in interface configuration mode. To disable IS-IS hello padding, use the `no` form of this command.

```
isis hello padding
no isis hello padding
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

IS-IS hello padding is enabled.

**Command Modes**

Interface configuration

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.0(5)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(5)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Intermediate System-to-Intermediate System (IS-IS) hellos are padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

You can disable hello padding in order to avoid wasting network bandwidth in case the MTU of both interfaces is the same or, in case of translational bridging. While hello padding is disabled, Cisco routers still send the first five IS-IS hellos padded to the full MTU size, in order to maintain the benefits of discovering MTU mismatches.

To selectively disable hello padding for a specific interface, enter the `no isis hello padding` command in interface configuration mode. To disable hello padding for all interfaces on a router for the IS-IS routing process, enter the `no hello padding` command in router configuration mode.

**Examples**

To turn off hello padding at the interface level for the Ethernet interface 0/0, enter the `no isis hello padding` command in interface configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface e0/0
Router(config-if)# no isis hello padding
Router(config-if)# end
```

When the `show clns neighbor` command is entered for Ethernet interface 0/0, the output confirms that hello padding has been turned off for both Level 1 and Level 2 circuit types:

```
Router_A# show clns interface e0/0
```
Ethernet0/0 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 47 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: Router_B.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: Router_B.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
      ! No hello padding
    Next IS-IS LAN Level-2 Hello in 2 seconds
      ! No hello padding

When the `debug isis adj packets` command is entered, the output will show the IS-IS hello protocol data unit (PDU) length when a hello packet has been sent to or received from an IS-IS adjacency. In the following example the IS-IS hello PDU length is 1497:

Router# debug isis adj packets e0/0

IS-IS Adjacency related packets debugging is on
Router# *Oct 11 18:04:17.455: ISIS-Adj: Sending L1 LAN IIH on Ethernet0/0, length 55
Oct 11 18:04:19.075: ISIS-Adj: Rec L2 IIH from aabb.cc00.6600 (Ethernet0/0), cir type
L1L2, cir id 0000.0000.000B.01, length 1497

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello padding</td>
<td>Displays information on all adjacency-related activity such as hello packets sent and received and IS-IS adjacencies going up and down.</td>
<td>Reenables IS-IS hello padding at the router level.</td>
</tr>
</tbody>
</table>
| `debug isis adj packets` | Lists the CLNS-specific information about each interface. | ```
| show clns interface | ```

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>The <code>minimal</code> keyword was added.</td>
</tr>
</tbody>
</table>

**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.

```plaintext
interface serial 0
isis hello-interval 5 level-1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isis hello-multiplier</td>
<td>Specifies the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down.</td>
</tr>
</tbody>
</table>
**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>isis hello padding</code></td>
<td>Specifies the length of time between hello packets that the Cisco IOS software sends.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isis retransmit-interval</td>
<td>Configures the time between retransmission of each LSP (IS-IS link-state PDU) over point-to-point links.</td>
</tr>
</tbody>
</table>
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.

\[
\text{isis mesh-group [number | blocked]}
\]

\[
\text{no isis mesh-group [number | blocked]}
\]

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>(Optional) A number identifying the mesh group of which this interface is a member.</td>
</tr>
<tr>
<td><code>blocked</code></td>
<td>(Optional) Specifies that no LSP flooding will take place on this subinterface.</td>
</tr>
</tbody>
</table>

### Defaults

The interface performs normal flooding.

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router isis</td>
<td>Enables the IS-IS routing protocol and specifies an IS-IS process.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>password</code></td>
<td>Authentication password you assign for an interface.</td>
</tr>
<tr>
<td><code>level-1</code></td>
<td>(Optional) Configures the authentication password for Level 1 independently.</td>
</tr>
<tr>
<td></td>
<td>For Level 1 routing, the router acts as a station router only.</td>
</tr>
<tr>
<td><code>level-2</code></td>
<td>(Optional) Configures the authentication password for Level 2 independently.</td>
</tr>
<tr>
<td></td>
<td>For Level 2 routing, the router acts as an area router only.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` keywords.

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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number-value</code></td>
<td>Sets the priority of a router and is a number from 0 to 127. The default value is 64.</td>
</tr>
<tr>
<td><code>level-1</code></td>
<td>(Optional) Sets the priority for Level 1 independently.</td>
</tr>
<tr>
<td><code>level-2</code></td>
<td>(Optional) Sets the priority for Level 2 independently.</td>
</tr>
</tbody>
</table>

**Defaults**

Priority of 64  
Level 1 and Level 2

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>isis lsp-interval</code></td>
<td>Configures the time delay between successive IS-IS LSP transmissions.</td>
</tr>
<tr>
<td><code>isis retransmit-throttle-interval</code></td>
<td>Configures the amount of time between retransmissions of any IS-IS LSPs on a point-to-point interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>isis lsp-interval</code></td>
<td>Configures the time delay between successive IS-IS LSP transmissions.</td>
</tr>
<tr>
<td><code>isis retransmit-interval</code></td>
<td>Configures the amount of time between retransmission of each IS-IS LSPs over a point-to-point link.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>level-1</th>
<th>(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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1-2</td>
<td>(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.</td>
</tr>
<tr>
<td>level-2-only</td>
<td>(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.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>This command was modified to include multiarea IS-IS routing.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>router isis</code></td>
<td>Enables the IS-IS routing protocol and specifies an IS-IS process.</td>
</tr>
<tr>
<td><code>show clns neighbor areas</code></td>
<td>Displays information about IS-IS neighbors and the areas to which they belong.</td>
</tr>
</tbody>
</table>
**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**

| 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 occurrences 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>isis lsp-interval</code></td>
<td>Sets the time delay between successive IS-IS LSP transmissions.</td>
</tr>
<tr>
<td><code>isis retransmit-interval</code></td>
<td>Sets the amount of time between retransmission of each IS-IS LSP on a point-to-point link.</td>
</tr>
<tr>
<td><code>isis retransmit-throttle-interval</code></td>
<td>Sets the minimum delay between retransmissions on each LSP on a point-to-point interface.</td>
</tr>
</tbody>
</table>
**Isp-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**

<table>
<thead>
<tr>
<th><strong>seconds</strong></th>
<th>Interval (in seconds) at which LSPs are refreshed. The range is 1 to 65535 seconds. The default value is 900 seconds (15 minutes).</th>
</tr>
</thead>
</table>

**Defaults**

900 seconds (15 minutes)

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>max-lsp-lifetime</code> (IS-IS)</td>
<td>Sets the maximum time that link-state packets (LSPs) can remain in a router’s database without being refreshed.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lsp-refresh-interval</code> (IS-IS)</td>
<td>Sets the link-state packet (LSP) refresh interval.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>This command was modified to include multiarea IS-IS routing.</td>
</tr>
</tbody>
</table>

**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.
The following example configures a router with system ID 0000.0c11.1111.00 and area ID 47.0004.004d.0001:

```
router isis CHEESNUT
  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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is-type</td>
<td>Configures the routing level for an instance of the IS-IS routing process.</td>
</tr>
<tr>
<td>router isis</td>
<td>Enables the IS-IS routing protocol and specifies an IS-IS process.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>area-tag</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
prrc-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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prc-max-wait</td>
<td>Indicates the maximum interval (in seconds) between two consecutive PRC calculations. Value range is 1 to 120 seconds. The default is 5 seconds.</td>
</tr>
<tr>
<td>prc-initial-wait</td>
<td>(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.</td>
</tr>
<tr>
<td>prc-second-wait</td>
<td>(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).</td>
</tr>
</tbody>
</table>

### Defaults

- prc-max-wait: 5 seconds
- prc-initial-wait: 2000 milliseconds
- prc-second-wait: 5000 milliseconds

### Command Modes

Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 Intermediate System-to-Intermediate System (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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>Multiarea functionality was added, changing the way the tag argument (now <code>area-tag</code>) is used.</td>
</tr>
</tbody>
</table>

### 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.

After you enter the `router isis` command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

**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 tag1
  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 CISCO is the value for the `area-tag` argument:

```
router isis CISCO
```

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 usage of the `maximum-paths` option:

```
router isis
maximum-paths?
20
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clns router isis</td>
<td>Enables IS-IS routing for ISO CLNS on an interface and attaches an area designator to the routing process.</td>
</tr>
<tr>
<td>ip router isis</td>
<td>Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.</td>
</tr>
<tr>
<td>net</td>
<td>Configures an IS-IS NET for the routing process.</td>
</tr>
<tr>
<td>redistribute (IP)</td>
<td>Redistribute routes from one routing domain into another routing domain.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another.</td>
</tr>
</tbody>
</table>
set-attached-bit

To specify constraints for when a Level 1 - Level 2 (L1L2) router should set its attached-bit, use the set-attached-bit route-map command in router configuration mode. To disable this function, use the no form of this command.

```
set-attached-bit route-map map-tag

no set-attached-bit route-map map-tag
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>route-map map-tag</code></td>
<td>(Required) Identifier of a configured route map. If the specified route map is matched, the router continues to set its attached-bit.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(4)B</td>
<td>This command was integrated into Cisco IOS Release 12.2(4)B.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In the current IS-IS implementation, as specified in ISO 10589, L1L2 routers set their Level 1 (L1) link-state packet (LSP) attached-bit when they see other areas in their own domain, or see other domains. However, in some network topologies, adjacent L1L2 routers in different areas may lose connectivity to the Level 2 (L2) backbone. Level 1 (L1) routers may then send traffic destined outside of the area or domain to L1L2 routers that may not have such connectivity.

To allow more control over the attached-bit setting for L1L2 routers, enter the `set-attached-bit` command in router configuration mode. The route map can specify one or more CLNS routes. If at least one of the match address route-map clauses matches a route in the L2 CLNS routing table, and if all other requirements for setting the attached-bit are met, the L1L2 router will continue to set the attached-bit in its L1 LSP. If the requirements are not met or no match address route-map clauses match a route in the L2 CLNS routing table, the attached-bit will not be set.

**Note**

Wildcarded matches are not supported. For each route-map statement, an exact route lookup of the specified route will be performed. The first matched route will have other match statements applied.
**Examples**

In the following example, the attached-bit will stay set when the router matches 49.00aa in the L2 CLNS routing table.

```
clns filter-set L2_backbone_connectivity permit 49.00aa
route-map check-for-L2_backbone_connectivity
match clns address L2_backbone_connectivity
router isis
  set-attached-bit route-map check-for-L2_backbone_connectivity
end
show clns route 49.00aa
```

Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
  via tr2, Serial0
    isis, route metric is 30, route version is 58

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another.</td>
</tr>
<tr>
<td>show clns route</td>
<td>Displays one or all of the destinations to which a router knows how to route CLNS packets.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.3(2)</td>
<td>The <code>on-startup</code> keyword and the <code>seconds</code> argument were added.</td>
</tr>
<tr>
<td>12.0(7)S</td>
<td>The <code>wait-for-bgp</code> keyword was added.</td>
</tr>
<tr>
<td>12.1(9)</td>
<td>The <code>wait-for-bgp</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(2)</td>
<td>The <code>wait-for-bgp</code> keyword was added.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>The <code>suppress</code>, <code>interlevel</code>, and <code>external</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(8)</td>
<td>The <code>suppress</code>, <code>interlevel</code>, and <code>external</code> keywords were added.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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`. 
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

<table>
<thead>
<tr>
<th>LSPID</th>
<th>LSP Seq Num</th>
<th>LSP Checksum</th>
<th>LSP Holdtime</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0C00.0C35.00-00 0x0000000C</td>
<td>0x5696</td>
<td>792</td>
<td>0/0/0</td>
<td></td>
</tr>
<tr>
<td>0000.0C00.40AF.00-00* 0x00000009</td>
<td>0x8452</td>
<td>1077</td>
<td>1/0/0</td>
<td></td>
</tr>
<tr>
<td>0000.0C00.62E6.00-00 0x0000000A</td>
<td>0x38E7</td>
<td>383</td>
<td>0/0/0</td>
<td></td>
</tr>
<tr>
<td>0000.0C00.62E6.00-00 0x0000000A</td>
<td>0x82E7</td>
<td>384</td>
<td>0/0/0</td>
<td></td>
</tr>
<tr>
<td>0800.2B16.24EA.00-00 0x0000000F</td>
<td>0x8864</td>
<td>1188</td>
<td>1/0/0</td>
<td></td>
</tr>
<tr>
<td>0800.2B16.24EA.00-00 0x0000000E</td>
<td>0x0935</td>
<td>1198</td>
<td>1/0/0</td>
<td></td>
</tr>
</tbody>
</table>

Table 25 describes the significant fields shown in the display.

**Table 25  show isis database Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSPID</td>
<td>The LSP identifier. The first six octets form the system ID of the router that originated the LSP.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For each LAN, the designated router for that LAN will create and flood a pseudonode LSP, describing all systems attached to that LAN.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>LSP Seq Num</td>
<td>Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.</td>
</tr>
<tr>
<td>LSP Checksum</td>
<td>Checksum of the entire LSP packet.</td>
</tr>
<tr>
<td>LSP Holdtime</td>
<td>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.</td>
</tr>
<tr>
<td>ATT</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 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 0x00000000 0x04C8 317 0/0/0
  Metric: 0 IS 0000.0C00.0C35.00
  --More--
  0000.0C00.3E51.00-00 0x00000009 0x9AB8 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Address:</td>
<td>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.</td>
</tr>
<tr>
<td>Metric:</td>
<td>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).</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Various addresses</td>
<td>The IP entries are the directly connected IP subnets the router is advertising (with associated metrics). The IP-External entry is a redistribute route.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the show isis lsp-log command:

Router# show isis lsp-log

<table>
<thead>
<tr>
<th>Level 1 LSP log</th>
<th>Interface</th>
<th>Triggers</th>
</tr>
</thead>
<tbody>
<tr>
<td>When</td>
<td>Count</td>
<td></td>
</tr>
<tr>
<td>07:05:18</td>
<td>3</td>
<td>CONFIG NEWADJ DIS</td>
</tr>
<tr>
<td>07:05:13</td>
<td>2</td>
<td>Ethernet0 NEWADJ DIS</td>
</tr>
<tr>
<td>07:04:43</td>
<td>1</td>
<td>ATTACHFLAG</td>
</tr>
<tr>
<td>07:01:38</td>
<td>2</td>
<td>Ethernet0 IPUP</td>
</tr>
<tr>
<td>07:01:33</td>
<td>2</td>
<td>Loopback0 CONFIG</td>
</tr>
<tr>
<td>07:01:24</td>
<td>1</td>
<td>Ethernet0 DELADJ</td>
</tr>
<tr>
<td>07:01:17</td>
<td>2</td>
<td>Ethernet0 DIS ES</td>
</tr>
<tr>
<td>07:01:02</td>
<td>1</td>
<td>Ethernet0 NEWADJ</td>
</tr>
<tr>
<td>07:00:57</td>
<td>2</td>
<td>Ethernet0 NEWADJ DIS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 2 LSP log</th>
<th>Interface</th>
<th>Triggers</th>
</tr>
</thead>
<tbody>
<tr>
<td>When</td>
<td>Count</td>
<td></td>
</tr>
<tr>
<td>07:05:24</td>
<td>2</td>
<td>CONFIG NEWADJ</td>
</tr>
<tr>
<td>07:05:23</td>
<td>1</td>
<td>Ethernet0 NEWADJ</td>
</tr>
<tr>
<td>07:05:18</td>
<td>1</td>
<td>Ethernet0 DIS</td>
</tr>
<tr>
<td>07:05:00</td>
<td>1</td>
<td>Serial0 NEWADJ</td>
</tr>
<tr>
<td>07:01:44</td>
<td>2</td>
<td>Ethernet0 IPUP</td>
</tr>
<tr>
<td>07:01:39</td>
<td>3</td>
<td>Loopback0 CONFIG DELADJ</td>
</tr>
<tr>
<td>07:01:30</td>
<td>1</td>
<td>Ethernet0 DELADJ</td>
</tr>
<tr>
<td>07:01:25</td>
<td>1</td>
<td>Serial0 NEWADJ</td>
</tr>
<tr>
<td>07:00:56</td>
<td>1</td>
<td>IPIA</td>
</tr>
<tr>
<td>07:00:47</td>
<td>2</td>
<td>AREASET IPIA</td>
</tr>
</tbody>
</table>

Table 28 describes the fields shown in the display.
Table 28  *show isis lsp-log* Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When</td>
<td>Time elapsed since the LSP was generated.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of events that took place at this time.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface that caused the LSP regeneration.</td>
</tr>
<tr>
<td>Triggers</td>
<td>Event that triggered the LSP to be flooded. Possible triggers for an LSP are as follows:</td>
</tr>
<tr>
<td></td>
<td>• AREASET—Active area set changed.</td>
</tr>
<tr>
<td></td>
<td>• ATTACHFLAG—Attached bit changed state.</td>
</tr>
<tr>
<td></td>
<td>• CLEAR—Some form of manual <code>clear</code> command was issued.</td>
</tr>
<tr>
<td></td>
<td>• CONFIG—Any configuration change.</td>
</tr>
<tr>
<td></td>
<td>• DELADJ—Adjacency went down.</td>
</tr>
<tr>
<td></td>
<td>• DIS—DIS changed or pseudonode changed.</td>
</tr>
<tr>
<td></td>
<td>• ES—End System adjacency changed.</td>
</tr>
<tr>
<td></td>
<td>• HIPPITY—LSPDB overload bit changed state.</td>
</tr>
<tr>
<td></td>
<td>• IF_DOWN—Needs a new LSP.</td>
</tr>
<tr>
<td></td>
<td>• IP_DEF_ORIG—Default information originate changed.</td>
</tr>
<tr>
<td></td>
<td>• IPDOWN—Directly connected IP prefix down.</td>
</tr>
<tr>
<td></td>
<td>• IP_EXTERNAL—Redistributed IP route appeared or gone.</td>
</tr>
<tr>
<td></td>
<td>• IPIA—Interarea IP route appeared or gone.</td>
</tr>
<tr>
<td></td>
<td>• IPUP—Directly connected IP prefix up.</td>
</tr>
<tr>
<td></td>
<td>• NEWADJ—New adjacency came up.</td>
</tr>
<tr>
<td></td>
<td>• REDIST—Redistributed level-2 CLNS route changed.</td>
</tr>
<tr>
<td></td>
<td>• RRR_INFO—RRR bandwidth resource information.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show isis spf-log` command:

```
Router# show isis spf-log

Level 1 SPF log

<table>
<thead>
<tr>
<th>When</th>
<th>Duration</th>
<th>Nodes</th>
<th>Count</th>
<th>Last trigger</th>
<th>LSP</th>
<th>Triggers</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:15:46</td>
<td>3124</td>
<td>40</td>
<td>1</td>
<td>milles.00-00</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:15:24</td>
<td>3216</td>
<td>41</td>
<td>5</td>
<td>milles.00-00</td>
<td>TLVCODE</td>
<td>NEWLSP</td>
</tr>
<tr>
<td>00:15:19</td>
<td>3096</td>
<td>41</td>
<td>1</td>
<td>deurze.00-00</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:14:54</td>
<td>3004</td>
<td>41</td>
<td>2</td>
<td>milles.00-00</td>
<td>ATTACHFLAG</td>
<td>LSPHEADER</td>
</tr>
<tr>
<td>00:14:49</td>
<td>3384</td>
<td>41</td>
<td>1</td>
<td>milles.00-01</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:14:23</td>
<td>2932</td>
<td>41</td>
<td>3</td>
<td>milles.00-00</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:05:18</td>
<td>3140</td>
<td>41</td>
<td>1</td>
<td>PERIODIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:03:54</td>
<td>3144</td>
<td>41</td>
<td>1</td>
<td>milles.01-00</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:03:49</td>
<td>2908</td>
<td>41</td>
<td>1</td>
<td>milles.01-00</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:03:28</td>
<td>3148</td>
<td>41</td>
<td>3</td>
<td>bakel.00-00</td>
<td>TLVCODE</td>
<td>TLVCONTENT</td>
</tr>
<tr>
<td>00:03:15</td>
<td>3054</td>
<td>41</td>
<td>1</td>
<td>milles.00-00</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:02:53</td>
<td>2958</td>
<td>41</td>
<td>1</td>
<td>mortel.00-00</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:02:48</td>
<td>3632</td>
<td>41</td>
<td>2</td>
<td>milles.00-00</td>
<td>NEWADJ</td>
<td>TLVCODE</td>
</tr>
<tr>
<td>00:02:23</td>
<td>2988</td>
<td>41</td>
<td>1</td>
<td>milles.00-01</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:02:18</td>
<td>3016</td>
<td>41</td>
<td>1</td>
<td>gemert.00-00</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:02:14</td>
<td>2932</td>
<td>41</td>
<td>1</td>
<td>bakel.00-00</td>
<td>TLVCONTENT</td>
<td></td>
</tr>
<tr>
<td>00:02:09</td>
<td>2988</td>
<td>41</td>
<td>2</td>
<td>bakel.00-00</td>
<td>TLVCONTENT</td>
<td></td>
</tr>
<tr>
<td>00:01:54</td>
<td>3228</td>
<td>41</td>
<td>1</td>
<td>milles.00-00</td>
<td>TLVCODE</td>
<td></td>
</tr>
<tr>
<td>00:01:38</td>
<td>3120</td>
<td>41</td>
<td>3</td>
<td>rips.03-00</td>
<td>TLVCONTENT</td>
<td></td>
</tr>
</tbody>
</table>
```
Table 29 describes the significant fields shown in the display.

**Table 29  show isis spf-log Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When</td>
<td>How long ago (in hours: minutes: seconds) a full SPF calculation occurred. The last 20 occurrences are logged.</td>
</tr>
<tr>
<td>Duration</td>
<td>Number of milliseconds required to complete this SPF run. Elapsed time is wall clock time, not CPU time.</td>
</tr>
<tr>
<td>Nodes</td>
<td>Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.</td>
</tr>
<tr>
<td>Count</td>
<td>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.</td>
</tr>
<tr>
<td>Last trigger LSP</td>
<td>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.</td>
</tr>
<tr>
<td>Triggers</td>
<td>A list of all reasons that triggered a full SPF calculation. For a list of possible triggers, see Table 30.</td>
</tr>
</tbody>
</table>

Table 30 lists possible triggers of a full SPF calculation.

**Table 30  Possible Triggers of Full SPF Calculation**

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTACHFLAG</td>
<td>This router is now attached to the Level 2 backbone or it has just lost contact to the Level 2 backbone.</td>
</tr>
<tr>
<td>ADMINDIST</td>
<td>Another administrative distance was configured for the IS-IS process on this router.</td>
</tr>
<tr>
<td>AREASET</td>
<td>Set of learned area addresses in this area changed.</td>
</tr>
<tr>
<td>BACKUPOVFL</td>
<td>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.</td>
</tr>
<tr>
<td>DBCHANGED</td>
<td>A clear isis * command was issued on this router.</td>
</tr>
<tr>
<td>IPBACKUP</td>
<td>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.</td>
</tr>
<tr>
<td>IPQUERY</td>
<td>A clear ip route command was issued on this router.</td>
</tr>
<tr>
<td>LSPEXPIRED</td>
<td>Some LSP in the link-state database (LSDB) has expired.</td>
</tr>
<tr>
<td>LSPHEADER</td>
<td>ATT/P/OL bits or is-type in an LSP header changed.</td>
</tr>
<tr>
<td>NEWADJ</td>
<td>This router has created a new adjacency to another router.</td>
</tr>
<tr>
<td>NEWAREA</td>
<td>A new area (via NET) was configured on this router.</td>
</tr>
</tbody>
</table>
### Table 30 Possible Triggers of Full SPF Calculation (continued)

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEWLEVEL</td>
<td>A new level (via is-type) was configured on this router.</td>
</tr>
<tr>
<td>NEWLSP</td>
<td>A new router or pseudonode appeared in the topology.</td>
</tr>
<tr>
<td>NEWMETRIC</td>
<td>A new metric was configured on an interface of this router.</td>
</tr>
<tr>
<td>NEWSYSID</td>
<td>A new system ID (via network entity title (NET)) was configured on this router.</td>
</tr>
<tr>
<td>PERIODIC</td>
<td>Typically, every 15 minutes a router runs a periodic full SPF calculation.</td>
</tr>
<tr>
<td>RTCLEARED</td>
<td>A <code>clear clns route</code> command was issued on this router.</td>
</tr>
<tr>
<td>TLVCODE</td>
<td>TLV code mismatch, indicating that different TLVs are included in the newest version of an LSP.</td>
</tr>
<tr>
<td>TLVCONTENT</td>
<td>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.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1</td>
<td>The <code>level-1</code> and <code>level-2</code> keywords and the <code>host-nsap</code> argument were added.</td>
</tr>
</tbody>
</table>

**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        Et0             00e0.b064.46ec
Router_B   10       Router_B        Et0             00e0.b064.46ec
```
IS-IS paths to level-2 routers

<table>
<thead>
<tr>
<th>System Id</th>
<th>Metric</th>
<th>Next-Hop</th>
<th>Interface</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router_A</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router_B</td>
<td>10</td>
<td>Router_B</td>
<td>Et0</td>
<td>00e0.b064.46ec</td>
</tr>
<tr>
<td>Router_C</td>
<td>20</td>
<td>Router_B</td>
<td>Et0</td>
<td>00e0.b064.46ec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router_D</td>
<td>Se0</td>
<td>DLCI 100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router_D</td>
<td>Se1</td>
<td><em>HDLC</em></td>
</tr>
<tr>
<td>Router_D</td>
<td>10</td>
<td>Router_D</td>
<td>Se0</td>
<td>DLCI 100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router_D</td>
<td>Se1</td>
<td><em>HDLC</em></td>
</tr>
</tbody>
</table>

Table 31 describes the fields shown in the display.

### Table 31  show isis topology Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Id</td>
<td>Identification value of the system listed in the Level 1 or Level 2 forwarding table.</td>
</tr>
<tr>
<td>Metric</td>
<td>IS-IS metric for the route.</td>
</tr>
<tr>
<td>Next-Hop</td>
<td>System ID of best-cost next-hop to listed address.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the next-hop system is known.</td>
</tr>
<tr>
<td>SNPA</td>
<td>Subnetwork point of attachment (MAC address) of next-hop.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show clns es-neighbors</td>
<td>Lists the ES neighbors that this router knows.</td>
</tr>
<tr>
<td>show clns is-neighbors</td>
<td>Displays IS-IS related information for IS-IS router adjacencies.</td>
</tr>
<tr>
<td>show clns neighbors</td>
<td>Displays both ES and IS neighbors.</td>
</tr>
<tr>
<td>show clns neighbor areas</td>
<td>Displays information about IS-IS neighbors and the areas to which they belong.</td>
</tr>
<tr>
<td>show clns route</td>
<td>Displays one or all of the destinations to which the router knows how to route CLNS packets.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>(Optional) Apply intervals to Level-1 areas only.</td>
</tr>
<tr>
<td>level-2</td>
<td>(Optional) Apply intervals to Level-2 areas only.</td>
</tr>
<tr>
<td>spf-max-wait</td>
<td>Indicates the maximum interval (in seconds) between two consecutive SPF calculations. The range is 1 to 120 seconds. The default is 10 seconds.</td>
</tr>
<tr>
<td>spf-initial-wait</td>
<td>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).</td>
</tr>
<tr>
<td>spf-second-wait</td>
<td>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).</td>
</tr>
</tbody>
</table>

**Defaults**

- `spf-max-wait`: 10 seconds
- `spf-initial-wait`: 5500 milliseconds
- `spf-second-wait`: 5500 milliseconds

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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, 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Summary address designated for a range of addresses.</td>
</tr>
<tr>
<td>mask</td>
<td>IP subnet mask used for the summary route.</td>
</tr>
<tr>
<td>level-1</td>
<td>Only routes redistributed into Level 1 are summarized with the configured address and mask value.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>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.</td>
</tr>
<tr>
<td>level-2</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Defaults

All redistributed routes are advertised individually.

### Command Modes

Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.
Integrated IS-IS Commands

**summary-address (IS-IS)**

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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Aggregate address.</td>
</tr>
<tr>
<td>mask</td>
<td>Aggregate mask.</td>
</tr>
<tr>
<td>as-set</td>
<td>(Optional) Generates autonomous system set path information.</td>
</tr>
<tr>
<td>summary-only</td>
<td>(Optional) Filters all more-specific routes from updates.</td>
</tr>
<tr>
<td>suppress-map</td>
<td>(Optional) Name of the route map used to select the routes to be suppressed.</td>
</tr>
<tr>
<td>advertise-map</td>
<td>(Optional) Name of the route map used to select the routes to create AS_SET origin communities.</td>
</tr>
<tr>
<td>attribute-map</td>
<td>(Optional) Name of the route map used to set the attribute of the aggregate route.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.1(20)CC</td>
<td>The <code>nlri unicast</code>, <code>nlri multicast</code>, and <code>nlri unicast multicast</code> keywords were added.</td>
</tr>
<tr>
<td>12.0(2)S</td>
<td>The <code>nlri unicast</code>, <code>nlri multicast</code>, and <code>nlri unicast multicast</code> keywords were added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>The <code>nlri unicast</code>, <code>nlri multicast</code>, and <code>nlri unicast multicast</code> keywords were removed.</td>
</tr>
<tr>
<td></td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>
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.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>neighbor distribute-list</td>
<td>Distribute BGP neighbor information in an access list.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
</tbody>
</table>
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
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
b **gp 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ip bgp ipv4</strong></td>
<td>Displays information about the TCP and BGP connections to neighbors.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0 S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0 ST</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
<tr>
<td>show ip bgp ipv4</td>
<td>Displays information about the TCP and BGP connections to neighbors.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
<tr>
<td>show ip bgp ipv4</td>
<td>Displays information about the TCP and BGP connections to neighbors.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>bgp cluster-id</td>
<td>Configures the cluster ID if the BGP cluster has more than one route reflector.</td>
</tr>
<tr>
<td>neighbor route-reflector-client</td>
<td>Configures the router as a BGP route reflector and configures the specified neighbor as its client.</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-id</td>
<td>Cluster ID of this router acting as a route reflector; maximum of 4 bytes.</td>
</tr>
</tbody>
</table>

**Defaults**

The router ID of the single route reflector in a cluster

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp client-to-client reflection</td>
<td>Restores route reflection from a BGP route reflector to clients.</td>
</tr>
<tr>
<td>neighbor route-reflector-client</td>
<td>Configures the router as a BGP route reflector and configures the specified neighbor as its client.</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
</tbody>
</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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>as-number</code></td>
<td>Autonomous system number that internally includes multiple autonomous systems.</td>
</tr>
</tbody>
</table>

| Defaults                                  | No confederation identifier is configured.                                   |

| Command Modes                             | Router configuration                                                       |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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.

```bash
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp confederation peers</td>
<td>Configures the autonomous systems that belong to the confederation.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>as-number</th>
<th>Autonomous system numbers for BGP peers that will belong to the confederation.</th>
</tr>
</thead>
</table>

**Defaults**

No BGP peers are identified as belonging to the confederation.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp confederation identifier</td>
<td>Specifies a BGP confederation identifier.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>half-life</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>reuse</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>suppress</strong></td>
<td>(Optional) A route is suppressed when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.</td>
</tr>
<tr>
<td><strong>max-suppress-time</strong></td>
<td>(Optional) Maximum time (in minutes) a route can be suppressed. The range is from 1 to 20000; the default is 4 times the <code>half-life</code>. If the <code>half-life</code> value is allowed to default, the maximum suppress time defaults to 60 minutes. When the <code>max-suppress-time</code> 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))</td>
</tr>
<tr>
<td><strong>route-map</strong></td>
<td>(Optional) Name of route map that controls where BGP route dampening is enabled.</td>
</tr>
<tr>
<td><strong>map-name</strong></td>
<td></td>
</tr>
</tbody>
</table>

**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
BGP Commands

**bgp dampening**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>clear ip bgp dampening</td>
<td>Clears BGP route dampening information and unsuppresses the suppressed routes.</td>
</tr>
<tr>
<td>clear ip bgp flap-statistics</td>
<td>Clears BGP flap statistics.</td>
</tr>
<tr>
<td>show ip bgp dampened-paths</td>
<td>Displays BGP dampened routes.</td>
</tr>
<tr>
<td>show ip bgp flap-statistics</td>
<td>Displays BGP flap statistics.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>neighbor activate</code></td>
<td>Enables the exchange of information with a neighboring router.</td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 IGP, 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
```

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 192.168.43.22 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
```

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, best 3
  192.168.43.3 from 192.168.43.3 (10.4.1.1)
    Origin IGP, metric 30, valid, external
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection or session.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
<tr>
<td>show ip bgp neighbors</td>
<td>Displays information about the TCP and BGP connections to neighbors.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1 CC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
<tr>
<td>12.0(1)</td>
<td>BGP neighbor changes are logged by default.</td>
</tr>
</tbody>
</table>

**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.
The following example logs neighbor changes for BGP in router configuration mode:

```bash
bgp router 100
bgp log-neighbor-changes
```

The following example logs neighbor changes for BGP in address family configuration mode:

```bash
bgp router 100
address-family ipv4 unicast
bgp log-neighbor-changes
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>eigrp log-neighbor-changes</td>
<td>Enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.</td>
</tr>
<tr>
<td>logging buffered</td>
<td>Logs messages to an internal buffer.</td>
</tr>
<tr>
<td>show ip bgp ipv4</td>
<td>Displays information about the TCP and BGP connections to neighbors.</td>
</tr>
<tr>
<td>show ip bgp neighbors</td>
<td>Displays information about BGP neighbors.</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the state of logging (syslog).</td>
</tr>
</tbody>
</table>
bgp maxas-limit

To configure Border Gateway Protocol (BGP) to discard routes that have a number of as-path segments that exceed the specified value, use the `bgp maxas-limit` command in router configuration mode. To return the router to default operation, use the `no` form of this command.

```
bgp maxas-limit number
no bgp maxas-limit
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Specifies the number of autonomous system segments. The value that can be entered for this argument is a number from 1 to 2000.</td>
</tr>
</tbody>
</table>

**Defaults**

The default value in Cisco IOS software for the `number` argument is 75.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(17)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(17)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `bgp maxas-limit` command is used to limit the number of as-path segments that are permitted in inbound routes. If a route is received with an as-path segment that exceeds the configured limit, the BGP routing process will discard the route.

**Examples**

In the following example, the maximum as-path segment length is set to 30:

```
Router(config)# router bgp 40000
Router(config-router-af)# bgp maxas-limit 30
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection or session.</td>
</tr>
</tbody>
</table>
bpg redistribute-internal

To allow the redistribution of iBGP routes into an interior gateway protocol such as IS-IS or OSPF, use the `bpg redistribute-internal` command in router configuration mode. To remove the `bpg 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.

```
bpg redistribute-internal

no bpg 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use of the `bpg 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
    bpg redistribute-internal

clear ip bgp *
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection or session.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip extcommunity-list</td>
<td>Creates an extended community access list.</td>
</tr>
</tbody>
</table>
bgp suppress-inactive

To keep routes that are not installed in the routing information base (RIB) from being advertised to peers, use the **bgp suppress-inactive** command in address family or router configuration mode.

```
bgp suppress-inactive
no bgp suppress inactive
```

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

**Defaults**
This command is disabled by default.

**Command Modes**
Address family
Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command is a toggle. Use the **bgp suppress-inactive** command to prevent routes that are not installed in the RIB from being advertised to peers. Use the **no bgp suppress-inactive** command to make BGP ignore RIB failures when advertising routes to peers.

**Examples**
In the following example, the **bgp suppress-inactive** command is configured:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# router bgp 1
Router(config-router)# bgp suppress-inactive
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection using BGP soft reconfiguration.</td>
</tr>
<tr>
<td>show ip bgp rib-failure</td>
<td>Display BGP routes that failed to install in the RIB table.</td>
</tr>
</tbody>
</table>
# 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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>*</code></td>
<td>Specifies that all current BGP sessions will be reset.</td>
</tr>
<tr>
<td><code>neighbor-address</code></td>
<td>Specifies that only the identified BGP neighbor will be reset.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Specifies that the specified BGP peer group will be reset.</td>
</tr>
<tr>
<td><code>soft</code></td>
<td>(Optional) Soft reset. Does not reset the session.</td>
</tr>
<tr>
<td>`in</td>
<td>out`</td>
</tr>
</tbody>
</table>

## Defaults

No reset is initiated.

## Command Modes

Privileged EXEC

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(6)T</td>
<td>The dynamic inbound soft reset capability was added.</td>
</tr>
<tr>
<td>12.0(2)S</td>
<td>The dynamic inbound soft reset capability was added.</td>
</tr>
</tbody>
</table>

## 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor soft-reconfiguration</td>
<td>Configures the Cisco IOS software to start storing updates.</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>(Optional) IP address of the network about which to clear dampening information.</td>
</tr>
<tr>
<td><code>network-mask</code></td>
<td>(Optional) Network mask applied to the <code>ip-address</code> argument.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bgp dampening</code></td>
<td>Enables BGP route dampening or changes various BGP route dampening factors.</td>
</tr>
<tr>
<td><code>show ip bgp dampened-paths</code></td>
<td>Displays BGP dampened routes.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>out</td>
</tr>
<tr>
<td>soft</td>
<td>(Optional) Triggers soft reconfiguration.</td>
</tr>
<tr>
<td>ipv4</td>
<td>ipv6</td>
</tr>
<tr>
<td>multicast</td>
<td>(Optional) Triggers reset of IPv4 or IPv6 multicast address family session.</td>
</tr>
<tr>
<td>unicast</td>
<td>(Optional) Triggers reset of IPv4, IPv6, or VPNv4 unicast family session.</td>
</tr>
</tbody>
</table>

**Defaults**

A reset is not initiated.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(2)S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection or session.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td><code>neighbor soft-reconfiguration</code></td>
<td>Configures the Cisco IOS software to start storing updates.</td>
</tr>
<tr>
<td><code>show ip bgp</code></td>
<td>Displays entries in the BGP routing table.</td>
</tr>
</tbody>
</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]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>(Optional) Clears flap statistics for a single entry at this IP address. If this argument is placed before <strong>flap-statistics</strong>, the router clears flap statistics for all paths from the neighbor at this address.</td>
</tr>
<tr>
<td>regexp regexp</td>
<td>(Optional) Clears flap statistics for all the paths that match the regular expression.</td>
</tr>
<tr>
<td>filter-list list-name</td>
<td>(Optional) Clears flap statistics for all the paths that pass the access list.</td>
</tr>
<tr>
<td>network-mask</td>
<td>(Optional) Network mask applied to the <strong>address</strong> argument.</td>
</tr>
</tbody>
</table>

**Defaults**

No statistics are cleared.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp dampening</td>
<td>Enables BGP route dampening or changes various BGP route dampening factors.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>Name of the BGP peer group to clear.</td>
</tr>
</tbody>
</table>

| Defaults           | No BGP peer group members are cleared.           |

| Command Modes      | Privileged EXEC                                  |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
<th>The following example clears all members from the BGP peer group named internal:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>Router# clear ip bgp peer-group internal</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>neighbor peer-group</td>
<td>Configures a BGP neighbor to be a member of a peer group.</td>
</tr>
<tr>
<td></td>
<td>(assigning members)</td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>distribute-list in (IP)</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>distribute-list out</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
<tr>
<td>ip prefix-list description</td>
<td>Adds a text description of a prefix list.</td>
</tr>
<tr>
<td>ip prefix-list sequence-number</td>
<td>Enables the generation of sequence numbers for entries in a prefix list.</td>
</tr>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
<tr>
<td>show ip bgp regexp</td>
<td>Displays information about a prefix list or prefix list entries.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>neighbor ebgp-multihop</td>
<td>Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.</td>
</tr>
<tr>
<td>network (BGP and multiprotocol BGP)</td>
<td>Specifies the list of networks for the BGP routing process.</td>
</tr>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
default-metric (BGP)

To set a default metric for routes redistributed into Border Gateway Protocol (BGP), use the `default-metric` command in address family or router configuration mode. To remove the configured value and return BGP to default operation, use the `no` form of this command.

```
default-metric number

no default-metric number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Default metric value applied to the redistributed route. The range of values for this argument is from 1 to 4294967295.</td>
</tr>
</tbody>
</table>

**Defaults**

The following is default behavior if this command is not configured or if the `no` form of this command is entered:

- The metric of redistributed interior gateway protocol (IGP) routes is set to a value that is equal to the interior BGP (iBGP) metric.
- The metric of redistributed connected and static routes is set to 0.

When this command is enabled, the metric for redistributed connected routes is set to 0.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode support was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `default-metric` command is used to set the metric value for routes redistributed into BGP with the `redistribute` command. A default metric can be configured to solve the problem of redistributing routes with incompatible metrics. Assigning the default metric will allow redistribution to occur.

This value is the Multi Exit Discriminator (MED) that is evaluated by BGP during the best path selection process. The MED is a non-transitive value that is processed only within the local autonomous system and adjacent autonomous systems. The default metric is not set if the received route has a MED value.

**Note**

When enabled, the `default-metric` command applies a metric value of 0 to redistributed connected routes. The `default-metric` command does not override metric values that are applied with the `redistribute` command.
In the following example, a metric of 1024 is set for routes redistributed into BGP from OSPF:

```bash
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)# default-metric 1024
Router(config-router-af)# redistribute ospf 10
Router(config-router-af)# end
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
**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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>external-distance</code></td>
<td>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. Accept table values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.</td>
</tr>
<tr>
<td><code>internal-distance</code></td>
<td>Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Accept table values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.</td>
</tr>
<tr>
<td><code>local-distance</code></td>
<td>Administrative distance for BGP local routes. Local routes are those networks listed with a <code>network</code> router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Accept table values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>external-distance</code>: 20</td>
</tr>
<tr>
<td><code>internal-distance</code>: 200</td>
</tr>
<tr>
<td><code>local-distance</code>: 200</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address family configuration</td>
</tr>
<tr>
<td>Router configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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:

```plaintext
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
</tbody>
</table>
To filter routes or networks received in incoming Border Gateway Protocol (BGP) updates, use the `distribute-list in` command in router configuration mode. To delete the distribute list and remove it from the running configuration file, use the `no` form of this command.

```
distribute-list acl-number | prefix list-name in

no distribute-list acl-number | prefix list-name in
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl-number</td>
<td>IP access list number. The access list defines which networks are to be received and which are to be suppressed in routing updates.</td>
</tr>
<tr>
<td>prefix list-name</td>
<td>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 prefixes in the prefix list.</td>
</tr>
</tbody>
</table>

**Note**

Interface type and number arguments may be displayed in the CLI depending on the installed version of Cisco IOS software. However, the interface arguments are not support in any software release.

**Defaults**

If this command is configured without a predefined access list, the distribute list will default to permitting all traffic.

**Command Modes**

Router configuration

**Note**

The `distribute-list in` command can be entered in address family configuration mode. However, address family configuration is not recommended and not supported.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>acl-number</code> arguments was added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>prefix list-name</code> argument was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `distribute-list in` command is used to filter incoming BGP updates. An access list must be defined prior to configuration of this command. In addition to access lists, prefix list can be used to filter based upon the prefix length, making it possible to filter either on the prefix list, the gateway, or both for incoming updates. The session must be reset with the `clear ip bgp` command before the distribute list will take effect. To suppress networks from being advertised in updates, use the `distribute-list out` command.
Note: We recommend that you use IP prefix lists (configured with the `ip prefix-list` command in global configuration mode) instead of distribute lists. IP prefix lists provide improved performance and are simpler to configure. Distribute list configuration will be removed from the CLI at a future date.

Note: Prefix lists and access lists are mutually exclusive when configuring a distribute list. We recommend that you do not use both the `prefix-list` and `access-list-name` arguments with the `distribute-list in` command.

Examples:

In the following example, a prefix list and distribute list are defined to configure the BGP routing process to accept traffic from only network 192.168.1.0 and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```plaintext
Router(config)# ip prefix-list RED deny 0.0.0.0/0 le 32
Router(config)# ip prefix-list RED permit 10.108.0.0/16
Router(config)# ip prefix-list RED permit 192.168.1.0/24
Router(config)#!
Router(config)# router bgp 50000
Router(config-router)# network 10.108.0.0
Router(config-router)# distribute-list prefix RED in
Router(config-router)# end
Router# clear ip bgp in
```

In the following example, an access list and a distribute list are defined to configure the BGP routing process to accept traffic from only network 192.168.1.0 and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```plaintext
Router(config)# access-list 1 permit 192.168.1.0
Router(config)# access-list 1 permit 10.108.0.0
Router(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Router(config)#!
Router(config)# router bgp 50000
Router(config-router)# network 10.108.0.0
Router(config-router)# distribute-list 1 in
Router(config-router)# end
Router# clear ip bgp in
```

Related Commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>Defines an IP access list.</td>
</tr>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection or session.</td>
</tr>
<tr>
<td>distribute-list out (BGP)</td>
<td>Suppresses networks from being advertised in outbound BGP updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
**distribute-list out (BGP)**

To suppress networks from being advertised in outbound Border Gateway Protocol (BGP) updates, use the `distribute-list out` command in router configuration mode. To delete the distribute list and remove it from the running configuration file, use the `no` form of this command.

```
distribute-list acl-number | prefix list-name out [protocol process-number | connected | static]
no distribute-list acl-number | prefix list-name out [protocol process-number | connected | static]
```

**Syntax Description**

- **acl-number**: IP access list number. The access list defines which networks are to be received and which are to be suppressed in routing updates.
- **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 prefixes in the prefix list.
- **protocol process-number**: Specifies the routing protocol to apply the distribution list. BGP, EIGRP, OSPF, and RIP are supported. The process number is entered for all routing protocols, except RIP. The process number is a value from 1 to 65535.
- **connected**: Specifies peers and networks learned through connected routes.
- **static**: Specifies peers and networks learned through static routes.

**Note**

Interface type and number arguments may be displayed in the CLI depending on the installed version of Cisco IOS software. However, the interface arguments are not supported in any software release.

**Defaults**

If this command is configured without a predefined access list, the distribute list will default to permitting all traffic.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>acl-number</code> argument was added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>prefix list-name</code> argument was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `distribute-list out` command is used to filter outbound BGP updates. An access list must be defined prior to configuration of this command. In addition to access lists, prefix list can be used to filter based upon the prefix length, making it possible to filter either on the prefix list, the gateway, or both for incoming updates. The session must be reset with the `clear ip bgp` command before the distribute list will take effect. To filter routes that are received in inbound updates, use the `distribute-list in` command.
Entering a protocol and/or process-number arguments causes the distribute list to be applied to only routes derived from the specified routing process. Addresses not specified in the distribute-list command will not be advertised in outgoing routing updates after a distribute list is configured.

Note

We recommend that you use IP prefix lists (configured with the ip prefix-list command in global configuration mode) instead of distribute lists. IP prefix lists provide improved performance and are simpler to configure. Distribute list configuration will be removed from the CLI at a future date.

Note

Prefix lists and access lists are mutually exclusive when configuring distribute lists. We recommend that you do not use both the prefix-list and access-list-name arguments with the distribute-list out command.

Examples

In the following example, an access list and a distribute list are defined to configure the BGP routing process to advertise only network 192.168.0.0. An outbound route refresh is initiated to activate the distribute-list.

Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Router(config)# 
Router(config)# router bgp 50000
Router(config-router)# distribute-list 1 out
Router(config-router)# end
Router# clear ip bgp out

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>Defines an IP access list.</td>
</tr>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection or session.</td>
</tr>
<tr>
<td>distribute-list in (BGP)</td>
<td>Filters routes and networks received in updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>Specifies the route map to be used as an export route map for the VRF.</td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default behavior.

**Command Modes**

VRF configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>import map</code></td>
<td>Configures an import route map for a VRF.</td>
</tr>
<tr>
<td><code>ip extcommunity-list</code></td>
<td>Creates an extended community list for BGP and controls access to it.</td>
</tr>
<tr>
<td><code>ip vrf</code></td>
<td>Configures a VRF routing table.</td>
</tr>
<tr>
<td><code>route-target</code></td>
<td>Creates a route-target extended community for a VRF.</td>
</tr>
<tr>
<td><code>show ip vrf</code></td>
<td>Displays the set of defined VRFs and associated interfaces.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th><strong>access-list-number</strong></th>
<th>Integer from 1 to 199 that indicates the regular expression access list number.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>permit</strong></td>
<td>Permits access for matching conditions.</td>
</tr>
<tr>
<td><strong>deny</strong></td>
<td>Denies access to matching conditions.</td>
</tr>
<tr>
<td><strong>as-regexp</strong></td>
<td>Autonomous system in the access list using a regular expression. Refer to the “Regular Expressions” appendix in the <em>Cisco IOS Terminal Services Configuration Guide</em> for information about forming regular expressions.</td>
</tr>
</tbody>
</table>

**Defaults**

No access lists are defined.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor distribute-list</td>
<td>Distributes BGP neighbor information as specified in an access list.</td>
</tr>
<tr>
<td>neighbor filter-list</td>
<td>Sets up a BGP filter.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
</tbody>
</table>
ip bgp fast-external-fallover

To enable per-interface fast external fallover, enter the `ip bgp fast-external-fallover` command in interface configuration mode. To revert back to the current behavior, use the `no` format of this command.

```
ip bgp fast-external-fallover [permit | deny]
no ip bgp fast-external-fallover [permit | deny]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>Allows per-interface fast external fallover.</td>
</tr>
<tr>
<td>deny</td>
<td>Prevents per-interface fast external fallover.</td>
</tr>
</tbody>
</table>

**Defaults**

Global fast external fallover.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0ST</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1</td>
<td>This command was integrated into Cisco IOS Release 12.1.</td>
</tr>
<tr>
<td>12.2</td>
<td>This command was integrated into Cisco IOS Release 12.2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you specify the `ip bgp fast-external-fallover` command with the `permit` or `deny` keyword, it overrides the global setting. If you enter the `no` format of the command, the global setting is in effect for this interface.

**Examples**

The following example enables per-interface fast-external-fallover on interface Ethernet 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip bgp fast-external-fallover permit
```
ip community-list

To create or configure a Border Gateway Protocol (BGP) community list and to control access to it, use the **ip community-list** command in **global configuration command**. To delete the community list, use the **no** form of this command.

```
ip community-list {standard | standard list-name} {deny | permit} {community-number} [AA:NN] [internet] [local-AS] [no-advertise] [no-export]} | {expanded | expanded list-name} {deny | permit} regexp
no ip community-list standard | expanded | {expanded | standard} list-name
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>standard</td>
<td>Configures a standard community list using a number from 1 to 99 to identify one or more permit or deny groups of communities.</td>
</tr>
<tr>
<td>standard list-name</td>
<td>Configures a named standard community list.</td>
</tr>
<tr>
<td>permit</td>
<td>Permits access for a matching condition.</td>
</tr>
<tr>
<td>deny</td>
<td>Denies access for a matching condition.</td>
</tr>
<tr>
<td>community-number</td>
<td>(Optional) Specifies a community as a 32-bit number from 1 to 4294967200. A single community can be entered or multiple communities can be entered, each separated by a space.</td>
</tr>
<tr>
<td>AA:NN</td>
<td>(Optional) Autonomous system number and network number entered in the 4-byte new community format. This value is configured with with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space.</td>
</tr>
<tr>
<td>internet</td>
<td>(Optional) Specifies the Internet community. Routes with this community are advertised to all peers (internal and external).</td>
</tr>
<tr>
<td>no-export</td>
<td>(Optional) Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised external peers.</td>
</tr>
<tr>
<td>local-as</td>
<td>(Optional) Specifies the local-as community. Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised external peers or to other subautonomous systems within a confederation.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>(Optional) Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external).</td>
</tr>
<tr>
<td>expanded</td>
<td>Configures an expanded community list number from 100 to 500 to identify one or more permit or deny groups of communities.</td>
</tr>
<tr>
<td>expanded list-name</td>
<td>Configures a named expanded community list.</td>
</tr>
<tr>
<td>regexp</td>
<td>Configures a regular expression that is used to specify a pattern to match against an input string.</td>
</tr>
</tbody>
</table>

**Note** Regular expressions can be used only with expanded community lists.
BGP Commands

ip community-list

Defaults

BGP community exchange is not enabled by default. It is enabled on a per-neighbor basis with the `neighbor send-community` command.

The Internet community is applied to all routes or prefixes by default, until any other community value is configured with this command or the `set community` command.

Once a permit value has been configured to match a given set of communities, the community list defaults to an implicit deny for all other community values.

Community values entered in the new format (AA:NN) are converted to 32-bit numbers if the `ip bgp-community new-format` command is not enabled on the local router.

Defaults

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>Support for the <code>local-as</code> community was introduced.</td>
</tr>
<tr>
<td>12.0(10)S</td>
<td>Named community list support was added.</td>
</tr>
<tr>
<td>12.0(16)ST</td>
<td>Named community list support was introduced.</td>
</tr>
<tr>
<td>12.1(9)E</td>
<td>Named community list support was integrated into Cisco IOS Release 12.1(9)E.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>Named community list support was integrated into Cisco IOS Release 12.2(8)T.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>The maximum number of expanded community list numbers was increased from 199 to 500.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>The maximum number of expanded community list numbers was increased from 199 to 500.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `ip community-list` command is used to configure BGP community filtering. BGP community values are configured as a 32-bit number (old format) or as a 4-byte number (new format). The new community format is enabled when the `ip bgp-community new-format` command is entered in global configuration mode. The new community format consists of a 4-byte value. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. Named and numbered community lists are supported. BGP community attribute exchange between BGP peers is enabled when the `neighbor send-community` command is configured for the specified neighbor. The BGP community attribute is defined in RFC-1997 and RFC-1998.

Standard Community Lists

Standard community lists are used to configure well-known communities and specific community numbers. A maximum of 16 communities can be configured in a standard community list. If you attempt to configure more than 16 communities, the trailing communities that exceed the limit are not processed or saved to the running configuration file.

Expanded Community Lists

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in.
Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the Regular Expressions appendix of the Cisco IOS Terminal Services Configuration Guide.

**Community List Processing**

When multiple values are configured in the same community list statement, a logical AND condition is created. All community values must match to satisfy an AND condition. When multiple values are configured in separate community list statements, a logical OR condition is created. The first list that matches a condition is processed.

**Examples**

In the following example, a standard community list is configured that permits routes that from network 10 in autonomous system 50000:

```
Router(config)# ip community-list 1 permit 50000:10
```

In the following example, a standard community list is configured that permits only routes from peers in the same autonomous system or from subautonomous system peers in the same confederation:

```
Router(config)# ip community-list 1 permit no-export
```

In the following example, a standard community list is configured to deny routes that carry communities from network 40 in autonomous system 65534 and from network 60 in autonomous system 65412. This example shows a logical AND condition; all community values must match in order for the list to be processed.

```
Router(config)# ip community-list 2 deny 65534:40 65412:60
```

In the following example, a named standard community list is configured that permits all routes within the local autonomous system or permits routes from network 20 in autonomous system 40000. This example shows a logical OR condition; the first match is processed.

```
Router(config)# ip community-list standard RED permit local-AS
Router(config)# ip community-list standard RED permit 40000:20
```

In the following example, an expanded community list is configured that will deny routes that carry communities from any private autonomous system:

```
Router(config)# ip community-list 500 deny _64[6-9][0-9][0-9]_ _65[0-9][0-9][0-9]
```

In the following example, a named expanded community list configured that denies routes from network 1 through 99 in autonomous system 50000:

```
Router(config)# ip community-list expanded BLUE deny 50000:[0-9][0-9]
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match community</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set comm-list delete</td>
<td>Removes communities from the community attribute of an inbound or outbound update.</td>
</tr>
</tbody>
</table>
## Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp community</td>
<td>Displays routes that belong to specified BGP communities.</td>
</tr>
<tr>
<td>show ip bgp regexp</td>
<td>Displays routes that match a locally configured regular expression.</td>
</tr>
</tbody>
</table>
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 [permit | deny] [regular-expression] [rt | soo extended-community-value]
```

```
o ip extcommunity-list
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>standard-list-number</code></td>
<td>Integer from 1 to 99 that identifies one or more permit or deny groups of extended communities.</td>
</tr>
<tr>
<td><code>expanded-list-number</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Permits access for a matching condition.</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>Denies access for a matching condition.</td>
</tr>
<tr>
<td><code>regular-expression</code></td>
<td>(Optional) An input string pattern to match against.</td>
</tr>
<tr>
<td><code>rt</code></td>
<td>(Optional) Specifies the route target (RT) extended community attribute. The <code>rt</code> keyword can be configured only with standard extended community lists and not expanded community lists.</td>
</tr>
<tr>
<td><code>soo</code></td>
<td>(Optional) Specifies the site of origin (SOO) extended community attribute. The <code>soo</code> keyword can be configured only with standard extended community lists and not expanded community lists.</td>
</tr>
</tbody>
</table>
| `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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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)# 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)*
```

The following example configures an expanded extended community list that permits advertisements that contain a route target extended community attribute beginning with the pattern 100:

```
Router(config)# ip extcommunity-list 101 permit RT:100:*
```

Note

For information about regular expressions and how to use them, see Regular Expressions.
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>export map</code></td>
<td>Configures an export route map for a VRF.</td>
</tr>
<tr>
<td><code>match community</code></td>
<td>Matches a BGP VPN extended community list.</td>
</tr>
<tr>
<td><code>set extcommunity</code></td>
<td>Sets BGP extended community attributes.</td>
</tr>
<tr>
<td><code>show ip extcommunity-list</code></td>
<td>Displays routes that are permitted by the extended community list.</td>
</tr>
<tr>
<td><code>show route-map</code></td>
<td>Displays configured route maps.</td>
</tr>
</tbody>
</table>
ip prefix-list

To create a prefix list or add a prefix-list entry, use the `ip prefix-list` command in global configuration mode. To delete a prefix-list entry, use the `no` form of this command.

```
ip prefix-list {list-name \ list-number} \ seq number \ {deny network/length \ permit network/length} \ {ge ge-length \ le le-length}
no ip prefix-list {list-name \ list-number} \ seq number \ {deny network/length \ permit network/length} \ {ge ge-length \ le le-length}
```

**Syntax Description**

| list-name | Configures a name to identify the prefix list. |
| list-number | Configures a number to identify the prefix list. |
| seq number | (Optional) Applies a sequence number to a prefix-list entry. The range of sequence numbers that can be entered is from 1 to 4294967294. If a sequence number is not entered when configuring this command, a default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5. |
| deny | Denies access for a matching condition. |
| permit | Permits access for a matching condition. |
| network/length | Configures the network address, and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 0 to 32. |
| ge ge-length | (Optional) Specifies the lesser value of a range (the “from” portion of the range description) by applying the `ge-length` argument to the range specified. The `ge-length` argument represents the minimum prefix length to be matched. |
| le le-length | (Optional) Specifies the greater value of a range (the “to” portion of the range description) by applying the `le-length` argument to the range specified. The `le-length` argument represents the maximum prefix length to be matched. |

**Note** The `ge` keyword represents the greater than or equal to operator. The `le` keyword represents the less than or equal to operator.

**Defaults**

No prefix lists are created.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(3)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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-number 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/length` argument. Exact match is assumed when neither `ge` nor `le` is specified. The range is assumed to be from `ge-length` to 32 if only the `ge` attribute is specified. The range is assumed to be from `len` to `le-length` if only the `le` attribute is specified.

A specified `ge-length` and/or `le-value` must satisfy the following condition:

\[
length < ge-length < le-length \leq 32
\]

Notes:

- If you use the `ip prefix-list` command with the `default-information originate` command to generate default routes, specify only IP address 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 ge 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 prefix 10.0.0.0/8:

```
ip prefix-list abc permit 10.0.0.0/8
```

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 192.168/8:

```
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip prefix-list</td>
<td>Resets the hit count of the prefix list entries.</td>
</tr>
<tr>
<td>ip prefix-list description</td>
<td>Adds a text description of a prefix list.</td>
</tr>
<tr>
<td>ip prefix-list sequence-number</td>
<td>Enables the generation of sequence numbers for entries in a prefix list.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributions routes of the specified type.</td>
</tr>
<tr>
<td>match ip address</td>
<td>Redistributions 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.</td>
</tr>
<tr>
<td>neighbor prefix-list</td>
<td>Distributes BGP neighbor information as specified in a prefix list.</td>
</tr>
<tr>
<td>show ip prefix-list</td>
<td>Displays information about a prefix list or prefix list entries.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>list name</th>
<th>Prefix list name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>sequence-number</td>
<td>Sequence number of the prefix list.</td>
</tr>
<tr>
<td>text</td>
<td>Text description of the prefix list.</td>
</tr>
</tbody>
</table>

### Defaults

There is no text description.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-name</code>, <code>type</code>, and <code>number</code> arguments were added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>prefix-list</code> argument was added.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip prefix-list</td>
<td>Resets the hit count of the prefix list entries.</td>
</tr>
<tr>
<td>distribute-list out</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
<tr>
<td>ip prefix-list sequence-number</td>
<td>Enables the generation of sequence numbers for entries in a prefix list.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>neighbor prefix-list</td>
<td>Distributes BGP neighbor information as specified in a prefix list.</td>
</tr>
<tr>
<td>show ip prefix-list</td>
<td>Displays information about a prefix list or prefix list entries.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
The following example disables the default automatic generation of sequence numbers for prefix list entries:

```
   no ip prefix-list sequence-number
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip prefix-list</td>
<td>Resets the hit count of the prefix list entries.</td>
</tr>
<tr>
<td>distribute-list in</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>distribute-list out</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
<tr>
<td>ip prefix-list sequence-number</td>
<td>Enables the generation of sequence numbers for entries in a prefix list.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>neighbor prefix-list</td>
<td>Distributes BGP neighbor information as specified in a prefix list.</td>
</tr>
<tr>
<td>show ip prefix-list</td>
<td>Displays information about a prefix list or prefix list entries.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>standard-list-number</code></td>
<td>Specifies a standard community list number from 1 to 99 that identifies one or more permit or deny groups of communities.</td>
</tr>
<tr>
<td><code>expanded-list-number</code></td>
<td>Specifies an expanded community list number from 100 to 199 that identifies one or more permit or deny groups of communities.</td>
</tr>
<tr>
<td><code>community-list-name</code></td>
<td>The community list name.</td>
</tr>
<tr>
<td><code>exact-match</code></td>
<td>(Optional) Indicates that an exact match is required. All of the communities and only those communities specified must be present.</td>
</tr>
</tbody>
</table>

### Defaults

No community list is matched by the route map.

### Command Modes

Route-map configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip community-list</td>
<td>Creates a community list for BGP and controls access to it.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>standard-list-number</code></td>
<td>A standard extended community list number from 1 to 99 that identifies one or more permit or deny groups of extended community attributes.</td>
</tr>
<tr>
<td><code>expanded-list-number</code></td>
<td>An expanded extended community list number from 100 to 500 that identifies one or more permit or deny groups of extended community attributes.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip extcommunity-list</td>
<td>Creates an extended community list for BGP and controls access to it.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol</td>
</tr>
<tr>
<td></td>
<td>into another.</td>
</tr>
<tr>
<td>set extcommunity</td>
<td>Sets BGP extended community attributes.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
<tr>
<td>show ip bgp filter-list</td>
<td>Displays routes that are permitted by the extended community list.</td>
</tr>
<tr>
<td>show route-map</td>
<td>Displays configured route maps.</td>
</tr>
</tbody>
</table>
**maximum-paths**

To configure the maximum number of parallel routes that an IP routing protocol will install into the routing table, use the `maximum-paths` command in router configuration or address family configuration mode. To restore the default value, use the `no` form of this command.

```
maximum-paths number [import number] | import number
no maximum-paths number | import number
```

**Syntax Description**

- `number` Specifies the number of routes to install to the routing table. See the usage guidelines for the number of paths that can be configured with this argument.
- `import number` (Optional) Specifies the number of redundant paths that can be configured as backup multipaths for a VRF. This keyword can only be configured under a VRF in address family configuration mode.

**Defaults**

Border Gateway Protocol (BGP) by default will install only one best path in the routing table. The default for all other IP routing protocols is four paths.

**Command Modes**

- Router configuration
- Address family configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(25)S</td>
<td>The <code>import</code> keyword was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>The <code>import</code> keyword was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>The <code>import</code> keyword was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `maximum-paths` command is used to set the number of parallel (equal-cost) routes that BGP will install in the routing table to configure multipath loadsharing. The number of paths that can be configured is determined by the version of Cisco IOS software. The following list shows current limits:

- Cisco IOS Release 12.0S based software: 8 paths
- Cisco IOS Release 12.3T based software: 16 paths
- Cisco IOS Release 12.2S based software: 32 paths

The `maximum-paths` command cannot be configured with the `maximum-paths eibgp` command for the same BGP routing process.
Configuring VRF Import Paths

A VRF will import only one path (best path) per prefix from the source VRF table, unless the prefix is exported with a different route-target. If the best path goes down, the destination will not be reachable until the next import event occurs, and then a new best path will be imported into the VRF table. The import event runs every 15 seconds by default.

The import keyword allows you to configure the VRF table to accept multiple redundant paths in addition to the best path. An import path is a redundant path, and it can have a next hop that matches an installed multipath. This feature should be used when there are multiple paths with identical next hops available to ensure optimal convergence times. A typical application of this feature is to configure redundant paths in a network that has multiple route reflectors for redundancy.

**Note**
Configuring redundant paths with the import keyword can increase CPU and memory utilization significantly, especially in a network where there are many prefixes to learn and a large number of configured VRFs. It is recommended that this feature is only configured as necessary and that the minimum number of redundant paths are configured (Typically, not more than two).

**Examples**

In the following example, the router is configured to install 2 parallel routes in the BGP routing table:

```
Router(config)# router bgp 40000
Router(config-router)# maximum-paths 2
```

In the following example, the router is configured to install 6 equal-cost routes and 2 import routes (backup) in the VRF routing table:

```
Router(config)# router bgp 40000
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# maximum-paths 6 import 2
```

In the following example, the router is configured to install 2 import routes in the VRF routing table:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf BLUE
Router(config-router-af)# maximum-paths import 2
```
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the number.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td>seconds</td>
<td>Time (in seconds) is specified by an integer from 0 to 600.</td>
</tr>
</tbody>
</table>

**Defaults**

30 seconds for external peers and 5 seconds for internal peers.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>neighbor peer-group (creating)</td>
<td>Creates a BGP peer group.</td>
</tr>
</tbody>
</table>
neighbor advertise-map

To install a Border Gateway Protocol (BGP) route as a locally originated route in the BGP routing table for conditional advertisement, use the `neighbor advertise-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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Specifies the IP address of the router that should receive conditional advertisements.</td>
</tr>
<tr>
<td><code>advertise-map</code></td>
<td>Specifies the name of the route map that will be advertised if the conditions of the exist map or nonexist map are met.</td>
</tr>
<tr>
<td><code>map-name</code></td>
<td>Specifies the name of the route map that will be advertised if the conditions of the exist map or nonexist map are met.</td>
</tr>
<tr>
<td><code>non-exist-map</code></td>
<td>Specifies the name of the route map that will be compared to the advertise map. If the condition is met and no match occurs, the route will be advertised. If a match occurs, then the condition is not met, and the route is withdrawn.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

Address family

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1CC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>This command was integrated into Cisco IOS Release 11.2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `neighbor advertise-map` router configuration command to conditionally advertise selected routes. The routes or prefixes that will be conditionally advertised are defined in 2 route-maps, an advertise map and a nonexist map. The route map associated with the nonexist 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 to the specified neighbor when the condition is met. When configuring a nonexist map, the condition is met when the prefix exists in the advertise map but does not exist in the nonexist map. If the condition is not met, the route is withdrawn and conditional advertisement does not occur. All routes that may be dynamically advertised or not advertised need to exist in the BGP routing table for conditional advertisement to occur.
Examples

The following address family configuration example configures BGP to conditionally advertise a prefix to the 10.1.1.1 neighbor using a nonexistent map. If the prefix exists in MAP3 but not MAP4, the condition is met and the prefix is advertised.

```
router bgp 5
  address-family ipv4 multicast
  neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>route-map</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
</tbody>
</table>
**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.

```plaintext
neighbor {ip-address | peer-group-name} default-originate [route-map map-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td><code>route-map map-name</code></td>
<td>(Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.</td>
</tr>
</tbody>
</table>

**Defaults**

No default route is sent to the neighbor.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>Modifications were added to permit extended access lists.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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):

```
routing 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:

```
routing 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>neighbor ebgp-multihop</td>
<td>Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td><code>text</code></td>
<td>Text (up to 80 characters) that describes the neighbor.</td>
</tr>
</tbody>
</table>

### Defaults

There is no description of the neighbor.

### Command Modes

Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0</td>
<td>The peer-group-name argument was added.</td>
</tr>
<tr>
<td>11.2</td>
<td>The access-list-name argument was added.</td>
</tr>
<tr>
<td>12.0</td>
<td>The prefix-list-name argument was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>access-list (IP standard)</td>
<td>Defines a standard IP access list.</td>
</tr>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>ip as-path access-list</td>
<td>Defines a BGP-related access list.</td>
</tr>
<tr>
<td>neighbor filter-list</td>
<td>Sets up a BGP filter.</td>
</tr>
<tr>
<td>neighbor peer-group (creating)</td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0</td>
<td>The <code>peer-group-name</code> argument was added.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>neighbor advertise-map</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>non-exist-map</code></td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td><code>neighbor peer-group (creating)</code></td>
<td>Specifies the list of networks for the BGP routing process.</td>
</tr>
<tr>
<td><code>network (BGP and multiprotocol BGP)</code></td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
<tr>
<td>12.1</td>
<td>The <code>weight</code> keyword was removed.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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:

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>ip as-path access-list</td>
<td>Defines a BGP-related access list.</td>
</tr>
<tr>
<td>match as-path</td>
<td>Match BGP autonomous system path access lists.</td>
</tr>
<tr>
<td>neighbor distribute-list</td>
<td>Distributes BGP neighbor information as specified in an access list.</td>
</tr>
<tr>
<td>neighbor peer-group (creating)</td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td>neighbor weight</td>
<td>Assigns a weight to a neighbor connection.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(4.4)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>show ip bgp neighbors</td>
<td>Displays information about BGP neighbors.</td>
</tr>
<tr>
<td>show ip bgp peer-group</td>
<td>Displays information about BGP peer groups.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td>maximum</td>
<td>Maximum number of prefixes allowed from this neighbor.</td>
</tr>
<tr>
<td>threshold</td>
<td>(Optional) Integer specifying at what percentage of <code>maximum</code> the router starts to generate a warning message. The range is from 1 to 100; the default is 75 (percent).</td>
</tr>
<tr>
<td>warning-only</td>
<td>(Optional) Allows the router to generate a log message when the <code>maximum</code> is exceeded, instead of terminating the peering.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default. There is no limit on the number of prefixes.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection using BGP soft reconfiguration.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the BGP-speaking neighbor.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Name of a BGP peer group.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0</td>
<td>The <code>peer-group-name</code> argument was added.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>neighbor peer-group (creating)</code></td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td><code>set ip next-hop (BGP)</code></td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
</tbody>
</table>
neighbor next-hop-unchanged

To enable an external BGP (eBGP) multihop peer to propagate the next hop unchanged, use the `neighbor next-hop-unchanged` command in address family or router configuration mode. To disable next hop propagation capabilities, use the `no` form of this command.

```
neighbor ip-address | peer-group-name next-hop-unchanged

no neighbor ip-address | peer-group-name next-hop-unchanged
```

**Syntax Description**

- `ip-address` The IP address of the next hop.
- `peer-group-name` The name of a BGP peer group that is the next hop.

**Defaults**

No default behavior or values

**Command Modes**

- Address family configuration
- Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(16)ST</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2</td>
<td>This command was integrated into Cisco IOS Release 12.2.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `neighbor next-hop-unchanged` command is used to configure the propagate the next hop unchanged for multihop eBGP peering sessions. This command should not be configured on a route reflector, and the `neighbor next-hop-self` command should not be used to modify the next hop attribute for a route reflector when this feature is enabled for a route reflector client.

This command can be used to perform the following tasks:

- Bring the route reflector into the forwarding path, which can be used with the iBGP Multipath Load Sharing feature to configure load balancing.
- Configure interprovider Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) by not modifying the next hop attribute when advertising routes to an eBGP peer.
- Turn off the next hop calculation for an eBGP peer. This feature is useful for configuring the end-to-end connection of a label-switched path.

**Caution**

Incorrectly setting BGP attributes for a route reflector can cause inconsistent routing, routing loops, or a loss of connectivity. Setting BGP attributes for a route reflector should be attempted only by an experienced network operator.
Examples

**Route Reflector Configuration**

In the following example, the local router is configured as a route reflector and configures the 10.0.0.100 multihop peer as a route reflector client. A route map is created to set the advertised next hop to 172.16.0.1.

```
Router(config)# route-map NEXTHOP
Router(config-route-map)# set ip next-hop 172.16.0.1
Router(config-route-map)# exit
Router(config)# router bgp 65534
Router(config-router)# neighbor 10.0.0.100 remote-as 65412
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.0.0.100 activate
Router(config-router-af)# neighbor 10.0.0.100 ebgp-multihop 255
Router(config-router-af)# neighbor 10.0.0.100 route-reflector-client
Router(config-router-af)# neighbor 10.0.0.100 route-map NEXTHOP out
Router(config-router-af)# end
```

**Route Reflector Client Configuration**

In the following example, the local router (route-reflector client) is configured to establish peering with the route reflector and to propagate the next hop unchanged:

```
Router(config)# router bgp 65412
Router(config-router)# neighbor 192.168.0.1 remote-as 65412
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 192.168.0.1 activate
Router(config-router-af)# neighbor 192.168.0.1 ebgp-multihop 255
Router(config-router-af)# neighbor 192.168.0.1 next-hop-unchanged
Router(config-router-af)# end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard IPv4 address prefixes.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard VPNv4 address prefixes.</td>
</tr>
<tr>
<td>neighbor ebgp-multihop</td>
<td>Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.</td>
</tr>
<tr>
<td>neighbor route-map</td>
<td>Applies a route map to incoming or outgoing routes.</td>
</tr>
<tr>
<td>neighbor route-reflector-client</td>
<td>Configures the router as a BGP route reflector and configures the specified neighbor as its client.</td>
</tr>
</tbody>
</table>
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 25 characters. 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 can cause authentication to fail.

**Defaults**

This command is disabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection.

When configuring MD5 authentication, you can enter a case-sensitive password of up to 25 characters. The string can contain any alphanumeric characters, including spaces. A password cannot be configured in the number-space-anything format. The space after the number can cause authentication to fail. You can also use any combination of the following symbolic characters along with alphanumeric characters:

```
` ~ ! @ # $ % ^ & * ( ) - _ = + \ | } \ ] { \[ " ' : ; / > < . ?
```

**Caution**

If the authentication string is configured incorrectly, the BGP peering session will not be established. We recommend that you enter the authentication string carefully and verify that the peering session is established after authentication is configured.

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
```

### Configuring an MD5 Password in an Established BGP Session

If you configure or change the password or key used for MD5 authentication between two BGP peers, the local router will not tear down the existing session after you configure the password. The local router will attempt to maintain the peering session using the new password until the BGP holddown timer expires. The default time period is 180 seconds. If the password is not entered or changed on the remote router before the holddown timer expires, the session will time out.

**Note**

Configuring a new timer value for the holddown timer will only take effect after the session has been reset. So, it is not possible to change the configuration of the holddown timer to avoid resetting the BGP session.

### Examples

The following example enables the authentication feature between this router and the BGP neighbor at 10.108.1.1. The password that must also be configured for the neighbor is `bla4u00=2nkq`. The remote peer must be configured before the holddown timer expires.

```
router bgp 109
neighbor 10.108.1.1 password bla4u00=2nkq
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor peer-group (creating)</td>
<td>Creates a BGP peer group.</td>
</tr>
</tbody>
</table>
**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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the BGP neighbor that belongs to the peer group specified by the <code>peer-group-name</code> argument.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Name of the BGP peer group to which this neighbor belongs.</td>
</tr>
</tbody>
</table>

**Defaults**

There are no BGP neighbors in a peer group.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>neighbor peer-group (creating)</td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td>neighbor shutdown</td>
<td>Disables a neighbor or peer group.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.1(20)CC</td>
<td>The <code>nlri unicast</code>, <code>nlri multicast</code>, and <code>nlri unicast multicast</code> keywords were added.</td>
</tr>
<tr>
<td>12.0(2)S</td>
<td>The <code>nlri unicast</code>, <code>nlri multicast</code>, and <code>nlri unicast multicast</code> keywords were added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>The <code>nlri unicast</code>, <code>nlri multicast</code>, and <code>nlri unicast multicast</code> keywords were removed. Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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.

```plaintext
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.

```plaintext
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
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>clear ip bgp peer-group</td>
<td>Removes all the members of a BGP peer group.</td>
</tr>
<tr>
<td>show ip bgp peer-group</td>
<td>Displays information about BGP peer groups.</td>
</tr>
</tbody>
</table>
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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>IP address of neighbor.</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>Name of a BGP peer group.</td>
<td></td>
</tr>
<tr>
<td>prefix-list-name</td>
<td>Name of a prefix list.</td>
<td></td>
</tr>
<tr>
<td>in</td>
<td>Access list is applied to incoming advertisements to that neighbor.</td>
<td></td>
</tr>
<tr>
<td>out</td>
<td>Access list is applied to outgoing advertisements to that neighbor.</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

No BGP neighbor is specified.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0</td>
<td>The <code>peer-group-name</code> argument was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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.
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>clear ip prefix-list</td>
<td>Resets the hit count of the prefix list entries.</td>
</tr>
<tr>
<td>ip as-path access-list</td>
<td>Defines a BGP-related access list.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
<tr>
<td>ip prefix-list description</td>
<td>Adds a text description of a prefix list.</td>
</tr>
<tr>
<td>ip prefix-list sequence-number</td>
<td>Enables the generation of sequence numbers for entries in a prefix list.</td>
</tr>
<tr>
<td>neighbor filter-list</td>
<td>Sets up a BGP filter.</td>
</tr>
<tr>
<td>neighbor remote-as</td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td>show ip bgp peer-group</td>
<td>Displays information about BGP peer groups.</td>
</tr>
<tr>
<td>show ip prefix-list</td>
<td>Displays information about a prefix list or prefix list entries.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0</td>
<td>The <code>peer-group-name</code> argument was added.</td>
</tr>
<tr>
<td>11.1(20)CC</td>
<td>The <code>nlri unicast</code>, <code>nlri multicast</code>, and <code>nlri unicast multicast</code> keywords were added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>The <code>nlri unicast</code>, <code>nlri multicast</code>, and <code>nlri unicast multicast</code> keywords were removed.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor remote-as</td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td>router bgp</td>
<td>Configures the BGP routing process.</td>
</tr>
</tbody>
</table>
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.

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0</td>
<td>The <code>peer-group-name</code> argument was added.</td>
</tr>
</tbody>
</table>

**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-AS2051# 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor remote-as</td>
<td>Allows entries to the BGP neighbor table.</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>neighbor remote-as</td>
<td>Creates a BGP peer group.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>bgp client-to-client reflection</td>
<td>Restores route reflection from a BGP route reflector to clients.</td>
</tr>
<tr>
<td>bgp cluster-id</td>
<td>Configures the cluster ID if the BGP cluster has more than one route reflector.</td>
</tr>
<tr>
<td>neighbor route-reflector-client</td>
<td>Configures the router as a BGP route reflector and configures the specified neighbor as its client.</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td><code>both</code></td>
<td>(Optional) Specifies that both standard and extended communities will be sent.</td>
</tr>
<tr>
<td><code>standard</code></td>
<td>(Optional) Specifies that only standard communities will be sent.</td>
</tr>
<tr>
<td><code>extended</code></td>
<td>(Optional) Specifies that only extended communities will be sent.</td>
</tr>
</tbody>
</table>

**Defaults**

No communities attribute is sent to any neighbor.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0</td>
<td>The <code>peer-group-name</code> argument was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address-family ipv4</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>address-family vpnv4</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>match community</code></td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td><code>neighbor remote-as</code></td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td><code>set community</code></td>
<td>Sets the BGP communities attribute.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor maximum-prefix</td>
<td>Controls how many prefixes can be received from a neighbor.</td>
</tr>
<tr>
<td>show ip bgp summary</td>
<td>Displays the status of all BGP connections.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection using BGP soft reconfiguration.</td>
</tr>
<tr>
<td>neighbor remote-as</td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td>show ip bgp neighbors</td>
<td>Display information about the TCP and BGP connections to neighbors.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 `holdtime` 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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the BGP-speaking neighbor.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td>route-map-name</td>
<td>Name of a route map.</td>
</tr>
</tbody>
</table>

**Defaults**

No routes are unsuppressed.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>aggregate-address</td>
<td>Creates an aggregate entry in a BGP routing table.</td>
</tr>
<tr>
<td>neighbor route-map</td>
<td>Applies a route map to inbound or outbound routes.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the BGP-speaking neighbor.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td><code>interface-type</code></td>
<td>Interface to be used as the source.</td>
</tr>
</tbody>
</table>

### Defaults

Best local address

### Command Modes

Router configuration

### Command History

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor remote-as</td>
<td>Creates a BGP peer group.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor remote-as</td>
<td>Creates a BGP peer group.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td><code>number</code></td>
<td>Weight to assign. Acceptable values are from 0 to 65535.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>neighbor distribute-list</td>
<td>Distributes BGP neighbor information as specified in an access list.</td>
</tr>
<tr>
<td>neighbor filter-list</td>
<td>Sets up a BGP filter.</td>
</tr>
<tr>
<td>neighbor remote-as</td>
<td>Creates a BGP peer group.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-number</td>
<td>Network that BGP or multiprotocol BGP will advertise.</td>
</tr>
<tr>
<td>mask</td>
<td>(Optional) Network or subnetwork mask. If the <code>mask</code> keyword is configured, then an exact match must exist in the routing table.</td>
</tr>
<tr>
<td>network-mask</td>
<td>(Optional) Network mask address.</td>
</tr>
<tr>
<td>route-map map-name</td>
<td>(Optional) Name of a route map.</td>
</tr>
</tbody>
</table>

### Defaults

No networks are specified.

### Command Modes

Address family configuration
Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>The limit of 200 network commands per BGP router was removed.</td>
</tr>
<tr>
<td>11.1(20)CC</td>
<td>The <code>nlri unicast</code>, <code>nlri multicast</code>, and <code>nlri unicast multicast</code> keywords were added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>The <code>nlri unicast</code>, <code>nlri multicast</code>, and <code>nlri unicast multicast</code> keywords were removed. Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

### 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:

```bash
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:

```bash
router bgp 65000
    address-family ipv4 multicast
    network 10.108.0.0
```

The following example shows the use of the `mask` keyword:

```bash
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address-family ipv4</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>address-family vpv4</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>default-information originate (BGP)</code></td>
<td>Allows the redistribution of network 0.0.0.0 into BGP.</td>
</tr>
<tr>
<td><code>network backdoor</code></td>
<td>Specifies a backdoor route to a BGP-learned prefix that provides better information about the network.</td>
</tr>
<tr>
<td><code>router bgp</code></td>
<td>Configures the BGP routing process.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>ip-address</th>
<th>IP address of the network to which you want a backdoor route.</th>
</tr>
</thead>
</table>

**Defaults**

No network is marked as having a back door.

**Command Modes**

Address family configuration

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>distance bgp</td>
<td>Allows the use of external, internal, and local administrative distances that could be a better route to a node.</td>
</tr>
<tr>
<td>network (BGP and multiprotocol BGP)</td>
<td>Specifies networks to be advertised by the BGP and multiprotocol BGP routing processes.</td>
</tr>
<tr>
<td>router bgp</td>
<td>Assigns an absolute weight to a BGP network.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th><strong>as-number</strong></th>
<th>Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</th>
</tr>
</thead>
</table>

### Defaults

No BGP routing process is enabled by default.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th><strong>Command</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>network (BGP and multiprotocol BGP)</td>
<td>Specifies the list of networks for the BGP routing process.</td>
</tr>
<tr>
<td>timers bgp</td>
<td>Adjusts BGP network timers.</td>
</tr>
</tbody>
</table>
```markdown
**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 }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>tag</th>
<th>Converts the tag of a route into an autonomous system path. Applies only when redistributing routes into BGP.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>prepend as-path-string</td>
<td>Appends the string following the keyword <code>prepend</code> to the autonomous system path of the route that is matched by the route map. Applies to inbound and outbound BGP route maps.</td>
</tr>
</tbody>
</table>

**Defaults**

Autonomous system path is not modified.

**Command Modes**

Route-map configuration

**Release**

<table>
<thead>
<tr>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
</tr>
<tr>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```bash
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:

```bash
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set origin (BGP)</td>
<td>Sets the BGP origin code.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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`).
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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).

```plaintext
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).

```plaintext
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip community-list</code></td>
<td>Creates a community list for BGP and control access to it.</td>
</tr>
<tr>
<td><code>match community</code></td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td><code>route-map (IP)</code></td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td><code>set comm-list delete</code></td>
<td>Removes communities from the community attribute of an inbound or outbound update.</td>
</tr>
<tr>
<td><code>show ip bgp community</code></td>
<td>Displays routes that belong to specified BGP communities.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>half-life</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>reuse</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>suppress</code></td>
<td>Suppresses a route when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.</td>
</tr>
<tr>
<td><code>max-suppress-time</code></td>
<td>Maximum time (in minutes) a route can be suppressed. The range is from 1 to 20000; the default is four times the <code>half-life</code> value. If the <code>half-life</code> value is allowed to default, the maximum suppress time defaults to 60 minutes.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set origin (BGP)</td>
<td>Sets the BGP origin code.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets the value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
<tr>
<td>show route-map</td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>rt</th>
<th>Specifies the route target (RT) extended community attribute.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>soo</td>
<td>Specifies the site of origin (SOO) extended community attribute.</td>
</tr>
<tr>
<td>extended-community-value</td>
<td>Specifies the value to be set. The value can be one of the following combinations:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• autonomous-system-number:network-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ip-address:network-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The colon is used to separate the autonomous system number and network number.</td>
<td></td>
</tr>
<tr>
<td>additive</td>
<td>(Optional) Adds a route target to the existing route target list without replacing any existing route targets.</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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.

```plaintext
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:

```plaintext
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip extcommunity-list</code></td>
<td>Creates an extended community list and controls access to it.</td>
</tr>
<tr>
<td><code>match extcommunity</code></td>
<td>Matches a BGP VPN extended community list.</td>
</tr>
<tr>
<td><code>route-map (IP)</code></td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td><code>route-target</code></td>
<td>Creates a route target extended community for a VRF.</td>
</tr>
<tr>
<td><code>show ip extcommunity-list</code></td>
<td>Displays routes that are permitted by the extended community list.</td>
</tr>
<tr>
<td><code>show route-map</code></td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the next hop to which packets are output. The next hop must be an adjacent router.</td>
</tr>
<tr>
<td>peer-address</td>
<td>(Optional) Sets the next hop to be the BGP peering address.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>The peer-address keyword was added.</td>
</tr>
</tbody>
</table>

**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
```
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**Note**

This command is not supported for redistributing routes into Border Gateway Protocol (BGP).
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igp</td>
<td>Remote Interior Gateway Protocol (IGP) system.</td>
</tr>
<tr>
<td>egp</td>
<td>Local Exterior Gateway Protocol (EGP) system.</td>
</tr>
<tr>
<td>as-number</td>
<td>Remote autonomous system number. This is an integer from 0 to 65535.</td>
</tr>
<tr>
<td>incomplete</td>
<td>Unknown heritage.</td>
</tr>
</tbody>
</table>

**Defaults**

Default origin, based on route in main IP routing table

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value in a route map configuration.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets the value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Weight value. It can be an integer from 0 to 65535.</td>
</tr>
</tbody>
</table>

**Defaults**

The weight is not changed by the specified route map.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
</tbody>
</table>
### BGP Commands

**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 Border Gateway Protocol (BGP) routing table, use the `show ip bgp` command in command in EXEC mode.

```
show ip bgp [ip-address [mask [longer-prefixes [injected] | shorter-prefixes [length]]] | oer-paths | prefix-list name | route-map name]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>(Optional) IP address entered to filter the output to display only a particular host or network in the BGP routing table.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>(Optional) Mask to filter or match hosts that are part of the specified network.</td>
</tr>
<tr>
<td><code>longer-prefixes</code></td>
<td>(Optional) Displays the specified route and all more specific routes.</td>
</tr>
<tr>
<td><code>injected</code></td>
<td>(Optional) Displays more specific prefixes injected into the BGP routing table.</td>
</tr>
<tr>
<td><code>shorter-prefix</code></td>
<td>(Optional) Displays the specified route and all less specific routes.</td>
</tr>
<tr>
<td><code>length</code></td>
<td>(Optional) Specifies the prefix length. The value for this argument is a number from 0 to 32.</td>
</tr>
<tr>
<td><code>oer-paths</code></td>
<td>(Optional) Displays OER controlled prefixes in the BGP routing table.</td>
</tr>
<tr>
<td><code>prefix-list name</code></td>
<td>(Optional) Filters the output based on the specified prefix list.</td>
</tr>
<tr>
<td><code>route-map name</code></td>
<td>(Optional) Filters the output based on the specified route map.</td>
</tr>
</tbody>
</table>

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>The display of prefix advertisement statistics was added.</td>
</tr>
<tr>
<td>12.0(6)T</td>
<td>The display of a message indicating support for route refresh capability was added.</td>
</tr>
<tr>
<td>12.0(14)T</td>
<td>The <code>prefix-list</code> and <code>route-map</code> keywords were added.</td>
</tr>
<tr>
<td>12.0(14)ST</td>
<td>The <code>shorter-prefixes</code> keyword was added. This keyword is available</td>
</tr>
<tr>
<td>12.2(2)T</td>
<td>The output of the <code>show ip bgp network</code> command was enhanced to display multipaths and a best path to the specified network.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>A new status code indicating stale routes was added to support BGP graceful restart.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>A new status code indicating stale routes was added to support BGP graceful restart.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>The <code>oer-paths</code> keyword was added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `show ip bgp` command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.
**oer-paths keyword**

BGP prefixes that are monitored and controlled by Optimized Edge Routing (OER) are displayed by entering the `show ip bgp` command with the `oer-paths` keyword.

### Examples

**show ip bgp example**

The following example output shows the BGP routing table:

```
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

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 10.1.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* 10.2.0.0</td>
<td>10.0.33.35</td>
<td>10</td>
<td>0</td>
<td>35</td>
<td>?</td>
</tr>
<tr>
<td>*&gt;</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* 10.0.0.0</td>
<td>10.0.33.35</td>
<td>10</td>
<td>0</td>
<td>35</td>
<td>?</td>
</tr>
<tr>
<td>*&gt;</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 192.168.0.0/16</td>
<td>10.0.33.35</td>
<td>10</td>
<td>0</td>
<td>35</td>
<td>?</td>
</tr>
</tbody>
</table>
```

Table 32 describes the significant fields shown in the display.

**Table 32  show ip bgp Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>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 history. *—The table entry is valid. &gt;—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>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 <strong>network</strong> 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.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Table 32  show ip bgp Field Descriptions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric</td>
<td>If shown, the value of the interautonomous system metric.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the <code>set local-preference</code> route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
<tr>
<td>(stale)</td>
<td>Indicates that the following path for the specified autonomous system is marked as “stale” during a graceful restart process.</td>
</tr>
</tbody>
</table>

**show ip bgp ip-address example**

The following example displays information about the 192.168.1.0 entry in the BGP routing table:

```
Router B# show ip bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 48
Paths: (2 available, best #2, table Default-IP-Routing-Table)
Multipath: eBGP
  Advertised to update-groups:
    1          2
200
  172.16.1.1 from 172.16.1.1 (10.1.1.1)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
    Extended Community: 0x0:0:0
    DMZ-Link Bw 278 kbytes
200
  172.16.2.2 from 172.16.2.2 (10.2.2.2)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
    Extended Community: 0x0:0:0
    DMZ-Link Bw 625 kbytes
```

Table 33 describes the significant fields shown in the display.

**Table 33  show ip bgp Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP routing table entry for...</td>
<td>IP address or network number of the routing table entry.</td>
</tr>
<tr>
<td>version...</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>Paths:</td>
<td>The number of available paths, and the number of installed best paths. This line dispays “Default-IP-Routing-Table” when the best path is installed in the IP routing table.</td>
</tr>
<tr>
<td>Multipath:</td>
<td>This field is displayed when multipath loadsharing is enabled. This field will indicate if the multipaths are iBGP or eBGP.</td>
</tr>
<tr>
<td>Advertised to update-groups:</td>
<td>The number of each update group for which advertisements are processed.</td>
</tr>
</tbody>
</table>
show ip bgp longer-prefixes example

The following is example output from the `show ip bgp` command entered with the `longer-prefixes` keyword:

```
Router# show ip bgp 10.92.0.0 255.255.0.0 longer-prefixes
```

```
BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 10.92.0.0</td>
<td>10.92.72.30</td>
<td>8896</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
</tr>
<tr>
<td>*&gt; 10.92.1.0</td>
<td>10.92.72.30</td>
<td>8796</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
</tr>
<tr>
<td>*&gt; 10.92.11.0</td>
<td>10.92.72.30</td>
<td>42482</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
</tr>
<tr>
<td>*&gt; 10.92.14.0</td>
<td>10.92.72.30</td>
<td>8796</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
</tr>
<tr>
<td>*&gt; 10.92.15.0</td>
<td>10.92.72.30</td>
<td>8696</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
</tr>
<tr>
<td>*&gt; 10.92.16.0</td>
<td>10.92.72.30</td>
<td>1400</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
</tr>
<tr>
<td>*&gt; 10.92.17.0</td>
<td>10.92.72.30</td>
<td>1400</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
</tr>
<tr>
<td>*&gt; 10.92.18.0</td>
<td>10.92.72.30</td>
<td>8876</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
</tr>
<tr>
<td>*&gt; 10.92.19.0</td>
<td>10.92.72.30</td>
<td>8876</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
</tr>
</tbody>
</table>
```

show ip bgp shorter-prefixes example

The following is example output from the `show ip bgp` command entered with the `shorter-prefixes` keyword. An 8 bit prefix length is specified.

```
Router# show ip bgp 172.16.0.0/16 shorter-prefixes 8
```

```
<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 172.16.0.0</td>
<td>10.0.0.2</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.0.0.2</td>
<td>0</td>
<td>200</td>
<td>?</td>
</tr>
</tbody>
</table>
```

show ip bgp prefix-list example

The following is example output from the `show ip bgp` command entered with the `prefix-list` keyword:

```
Router# show ip bgp prefix-list ROUTE
```

```
BGP table version is 39, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```
### show ip bgp

The following is example output from the `show ip bgp` command entered with the `route-map` keyword:

```
Router# show ip bgp route-map LEARNED_PATH
BGP table version is 40, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td></td>
</tr>
</tbody>
</table>
```

### show ip bgp route-map example

The following is example output from the `show ip bgp` command entered with the `route-map` keyword:

```
Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0   10.0.0.2                               0 ?
*                   10.0.0.2                 0             0 200 ?
```
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 192.168.0.0/8</td>
<td>172.16.72.24</td>
<td></td>
<td>0</td>
<td>1878</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 172.16.0.0/16</td>
<td>172.16.72.30</td>
<td></td>
<td>0</td>
<td>108</td>
<td>?</td>
</tr>
</tbody>
</table>
```

Table 34 describes the significant fields shown in the display.

**Table 34  show ip bgp cidr-only Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version is 220</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>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. &gt;—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.</td>
</tr>
</tbody>
</table>
Table 34  show ip bgp cidr-only Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin codes</td>
<td>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.</td>
</tr>
<tr>
<td>Network</td>
<td>Internet address of the network the entry describes.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, the value of the interautonomous system metric.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the set local-preference route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>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.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community-number</td>
<td>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.</td>
</tr>
<tr>
<td>exact</td>
<td>(Optional) Displays only routes that have the same specified communities.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>The local-as community was added.</td>
</tr>
</tbody>
</table>

**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 ?
  *> 172.43.44.32   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 35 describes the significant fields shown in the display.  

**Table 35  show ip bgp community Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
</tbody>
</table>
### Table 35  show ip bgp community Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status codes</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>s—The table entry is suppressed.</td>
</tr>
<tr>
<td></td>
<td>*—The table entry is valid.</td>
</tr>
<tr>
<td></td>
<td>&gt;—The table entry is the best entry to use for that network.</td>
</tr>
<tr>
<td></td>
<td>i—The table entry was learned via an internal BGP (iBGP) session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a <strong>network</strong> router configuration command.</td>
</tr>
<tr>
<td></td>
<td>e—Entry originated from an Exterior Gateway Protocol (EGP).</td>
</tr>
<tr>
<td></td>
<td>?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, this is the value of the interautonomous system metric. This field is frequently not used.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the <strong>set local-preference</strong> route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Community list number in the range from 1 to 99.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Displays only routes that have an exact match.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* i3.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 1239 ?</td>
</tr>
<tr>
<td>*i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 1239 ?</td>
</tr>
<tr>
<td>*i6.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 568 ?</td>
</tr>
<tr>
<td>*i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 568 ?</td>
</tr>
<tr>
<td>*i7.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 35 ?</td>
</tr>
<tr>
<td>*i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 35 ?</td>
</tr>
<tr>
<td>*</td>
<td>193.16.72.24</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 i</td>
</tr>
<tr>
<td>*i8.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 560 ?</td>
</tr>
<tr>
<td>*i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 560 ?</td>
</tr>
<tr>
<td>*</td>
<td>193.16.72.24</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 560 ?</td>
</tr>
<tr>
<td>*i13.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 200 ?</td>
</tr>
<tr>
<td>*i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 200 ?</td>
</tr>
<tr>
<td>*</td>
<td>193.16.72.24</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 200 i</td>
</tr>
<tr>
<td>*i15.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 174 ?</td>
</tr>
<tr>
<td>*i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 174 ?</td>
</tr>
<tr>
<td>*i16.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 i</td>
</tr>
<tr>
<td>*i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 i</td>
</tr>
<tr>
<td>*</td>
<td>193.16.72.24</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 704 701 i</td>
</tr>
</tbody>
</table>
Table 36 describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>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. &gt;—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>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.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, this is the value of the interautonomous system metric. This field is frequently not used.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the set local-preference route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Network</th>
<th>From</th>
<th>Reuse</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*d 10.0.0.0</td>
<td>171.69.232.177</td>
<td>00:18:4</td>
<td>100</td>
</tr>
<tr>
<td>*d 12.0.0.0</td>
<td>171.69.232.177</td>
<td>00:28:5</td>
<td>100</td>
</tr>
</tbody>
</table>
```

Table 37 describes the significant fields shown in the display.

**Table 37  show ip bgp dampened-paths Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router</td>
<td>IP address of the router where route dampening is enabled.</td>
</tr>
<tr>
<td>*d</td>
<td>Route to the network indicated is dampened.</td>
</tr>
<tr>
<td>From</td>
<td>IP address of the peer that advertised this path.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Time (in hours:minutes:seconds) after which the path will be made available.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system path of the route that is being dampened.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp dampening</td>
<td>Enables BGP route dampening or changes various BGP route dampening factors.</td>
</tr>
<tr>
<td>clear ip bgp dampening</td>
<td>Clears BGP route dampening information and unsuppresses the suppressed routes.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 38 describes the significant fields shown in the display.

### Table 38  show ip bgp filter-list Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever</td>
</tr>
<tr>
<td></td>
<td>the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>Status of the table entry. The status is displayed at the beginning of</td>
</tr>
<tr>
<td></td>
<td>each line in the table. It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>s—The table entry is suppressed.</td>
</tr>
<tr>
<td></td>
<td>*—The table entry is valid.</td>
</tr>
<tr>
<td></td>
<td>&gt;—The table entry is the best entry to use for that network.</td>
</tr>
<tr>
<td></td>
<td>i—The table entry was learned via an internal BGP (iBGP) session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>Origin of the entry. The origin code is placed at the end of each line in</td>
</tr>
<tr>
<td></td>
<td>the table. It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>i—Entry originated from an Interior Gateway Protocol (IGP) and was</td>
</tr>
<tr>
<td></td>
<td>advertised with a <strong>network</strong> router configuration command.</td>
</tr>
<tr>
<td></td>
<td>e—Entry originated from an Exterior Gateway Protocol (EGP).</td>
</tr>
<tr>
<td></td>
<td>?—Origin of the path is not clear. Usually, this is a router that is</td>
</tr>
<tr>
<td></td>
<td>redistributed into BGP from an IGP.</td>
</tr>
<tr>
<td>Network</td>
<td>Internet address of the network the entry describes.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next system that is used when forwarding a packet to</td>
</tr>
<tr>
<td></td>
<td>the destination network. An entry of 0.0.0.0 indicates that the router</td>
</tr>
<tr>
<td></td>
<td>has some non-BGP route to this network.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, this is the value of the interautonomous system metric. This</td>
</tr>
<tr>
<td></td>
<td>field is frequently not used.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the set local-preference route-map</td>
</tr>
<tr>
<td></td>
<td>configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry</td>
</tr>
<tr>
<td></td>
<td>in this field for each autonomous system in the path. At the end of the</td>
</tr>
<tr>
<td></td>
<td>path is the origin code for the path:</td>
</tr>
<tr>
<td></td>
<td>i—The entry was originated with the IGP and advertised with a <strong>network</strong></td>
</tr>
<tr>
<td></td>
<td>router configuration command.</td>
</tr>
<tr>
<td></td>
<td>e—The route originated with EGP.</td>
</tr>
<tr>
<td></td>
<td>?—The origin of the path is not clear. Usually this is a path that is</td>
</tr>
<tr>
<td></td>
<td>redistributed into BGP from an IGP.</td>
</tr>
</tbody>
</table>
# 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>regexp regexp</td>
<td>(Optional) Clears flap statistics for all the paths that match the regular expression.</td>
</tr>
<tr>
<td>filter-list access-list</td>
<td>(Optional) Clears flap statistics for all the paths that pass the access list.</td>
</tr>
<tr>
<td>ip-address mask</td>
<td>(Optional) Clears flap statistics for a single entry at this IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>(Optional) Network mask applied to the value.</td>
</tr>
<tr>
<td>longer-prefix</td>
<td>(Optional) Displays flap statistics for more specific entries.</td>
</tr>
</tbody>
</table>

## Command Modes

EXEC

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## 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 39 describes the significant fields shown in the display.

## Table 39  `show ip bgp flap-statistics` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router where route dampening is enabled.</td>
</tr>
<tr>
<td>Network</td>
<td>Route to the network indicated is dampened.</td>
</tr>
</tbody>
</table>
Table 39  show ip bgp flap-statistics Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>IP address of the peer that advertised this path.</td>
</tr>
<tr>
<td>Flaps</td>
<td>Number of times the route has flapped.</td>
</tr>
<tr>
<td>Duration</td>
<td>Time (in hours:minutes:seconds) since the router noticed the first flap.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Time (in hours:minutes:seconds) after which the path will be made available.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system path of the route that is being dampened.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp dampening</td>
<td>Enables BGP route dampening or changes various BGP route dampening factors.</td>
</tr>
<tr>
<td>clear ip bgp flap-statistics</td>
<td>Clears BGP flap statistics.</td>
</tr>
</tbody>
</table>
show ip bgp inconsistent-as

To display routes with inconsistent originating autonomous systems, use the `show ip bgp inconsistent-as` command in EXEC mode.

```plaintext
show ip bgp inconsistent-as
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show ip bgp inconsistent-as` command in privileged EXEC mode:

```plaintext
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

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 11.0.0.0</td>
<td>171.69.232.55</td>
<td>0</td>
<td>300</td>
<td>88 90 99 ?</td>
</tr>
<tr>
<td>* 171.69.0.0</td>
<td>171.69.232.55</td>
<td>2222</td>
<td>0</td>
<td>300 90 99 88 200 ?</td>
</tr>
<tr>
<td>* 200.200.199.0</td>
<td>171.69.232.55</td>
<td>0</td>
<td>300</td>
<td>88 90 99 200 ?</td>
</tr>
<tr>
<td>* 171.69.232.52</td>
<td>2222</td>
<td>0</td>
<td>400</td>
<td>?</td>
</tr>
<tr>
<td>* 171.69.232.52</td>
<td>2222</td>
<td>0</td>
<td>400</td>
<td>?</td>
</tr>
</tbody>
</table>
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 40 describes the significant fields shown in the display.

**Table 40  show ip bgp ipv4 unicast Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
</tbody>
</table>
### Table 40  show ip bgp ipv4 unicast Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status codes</td>
<td>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. &gt;—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>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.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, the value of the interautonomous system metric.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the set local-preference route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
</tbody>
</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 [all] [ip-address [advertised-routes | dampened-routes | paths [regexp] | received prefix-filter | received-routes | routes]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>(Optional) Displays neighbor information for all address families. Only IPv4 neighbor information is displayed if this keyword is not entered.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>(Optional) IP address of a neighbor. If this argument is omitted, all neighbors are displayed.</td>
</tr>
<tr>
<td><code>advertised-routes</code></td>
<td>(Optional) Displays all routes that have been advertised to neighbors.</td>
</tr>
<tr>
<td><code>received-routes</code></td>
<td>(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.</td>
</tr>
<tr>
<td><code>routes</code></td>
<td>(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the <code>received-routes</code> keyword.</td>
</tr>
<tr>
<td><code>paths regexp</code></td>
<td>(Optional) Displays received paths. A regular expression can be used to filter the output.</td>
</tr>
<tr>
<td><code>dampened-routes</code></td>
<td>(Optional) Displays the dampened routes to the specified neighbor.</td>
</tr>
<tr>
<td><code>received prefix-filter</code></td>
<td>(Optional) Displays the prefix-list (outbound route filter [ORF]) sent from the specified neighbor.</td>
</tr>
</tbody>
</table>

### Command Default

The output of this command displays information for only IPv4 address family sessions if the `all` keyword is not entered.

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>received-routes</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(4)T</td>
<td>The <code>received prefix-filter</code> keyword was added.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>The output was enhanced to display MPLS label information.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>• This command was integrated into Cisco IOS Release 12.0(22)S. Support for the Cisco 12000 series routers (Engine 0 and Engine 2) was added.</td>
</tr>
<tr>
<td></td>
<td>• The <code>received prefix-filter</code> keyword was added.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The `show ip bgp neighbors` command is used to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance. This command displays information only about IPv4 address-family sessions unless the `all` keyword is entered.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

Examples

**show ip bgp neighbors example**

The following example shows the 10.108.50.2 neighbor. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
Router# show ip bgp neighbors 10.108.50.2
```

```
BGP neighbor is 10.108.50.2, remote AS 1, internal link
   BGP version 4, remote router ID 192.168.252.252
   BGP state = Established, up for 00:24:25
   Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is 60 seconds
   Neighbor capabilities:
      Route refresh: advertised and received(old & new)
      Graceful Restart Capability: advertised and received
      Address family IPv4 Unicast: advertised and received
   Message statistics:
      InQ depth is 0
      OutQ depth is 0
      Sent     Rcvd
      Opens:     3    3
      Notifications: 0    0
      Updates:    0    0
      Keepalives: 113  112
      Route Refresh: 0    0
      Total:      116  115
   Default minimum time between advertisement runs is 5 seconds
   For address family: IPv4 Unicast
      BGP table version 1, neighbor version 1/0
      Output queue size : 0
      Index 1, Offset 0, Mask 0x2
      1 update-group member
      Prefix activity:
         Sent     Rcvd
         Prefixes Current: 0     0
         Prefixes Total:   0     0
         Implicit Withdraw: 0    0
         Explicit Withdraw: 0    0
         Used as bestpath: n/a  0
         Used as multipath: n/a  0
      Outbound     Inbound
      Local Policy Denied Prefixes:
         Total: 0    0
   Number of NLRIs in the update sent: max 0, min 0
   Connections established 3; dropped 2
   Last reset 00:24:26, due to Peer closed the session
   Connection state is ESTAB, I/O status: 1, unread input bytes: 0
   Connection is ECN Disabled
```
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):

<table>
<thead>
<tr>
<th>Timer</th>
<th>Starts</th>
<th>Wakeups</th>
<th>Next</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrans</td>
<td>27</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>TimeWait</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>AckHold</td>
<td>27</td>
<td>18</td>
<td>0x0</td>
</tr>
<tr>
<td>SendWnd</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>KeepAlive</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>GiveUp</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>PmtuAger</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>DeadWait</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
</tbody>
</table>

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016  sndwnd: 15826
irs: 233567076  rcvnxt: 233567616  rcvwnd: 15845  delrcvwnd: 539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08

Table 41 describes the significant fields shown in the display. Fields that are preceded by the asterisk character are displayed only when the counter has a non-zero value.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>IP address of the BGP neighbor and its autonomous system number.</td>
</tr>
<tr>
<td>remote AS</td>
<td>Autonomous-system number of the neighbor.</td>
</tr>
<tr>
<td>internal link</td>
<td>“internal link” is displayed for iBGP neighbors. “external link” is displayed for external BGP (eBGP) neighbors.</td>
</tr>
<tr>
<td>BGP version</td>
<td>BGP version being used to communicate with the remote router.</td>
</tr>
<tr>
<td>remote router ID</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>BGP state</td>
<td>Finite state machine (FSM) stage of session negotiation.</td>
</tr>
<tr>
<td>up for</td>
<td>Time, in seconds, that the underlying TCP connection has been in existence.</td>
</tr>
<tr>
<td>Last read</td>
<td>Time since BGP last received a message from this neighbor.</td>
</tr>
<tr>
<td>last write</td>
<td>Time since BGP last sent a message to this neighbor.</td>
</tr>
<tr>
<td>hold time</td>
<td>Time, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.</td>
</tr>
<tr>
<td>keepalive interval</td>
<td>Time, interval in seconds, that keepalive messages are transmitted to this neighbor.</td>
</tr>
<tr>
<td>Neighbor capabilities</td>
<td>BGP capabilities advertised and received from this neighbor. “Advertised and received” is displayed when a capability is successfully exchanged between two routers.</td>
</tr>
</tbody>
</table>
**Table 41  show ip bgp neighbors Field Descriptions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Refresh</td>
<td>Status of the route refresh capability.</td>
</tr>
<tr>
<td>Graceful Restart Capability</td>
<td>Status of the graceful restart capability.</td>
</tr>
<tr>
<td>Address family IPv4 Unicast</td>
<td>IP Version 4 unicast-specific properties of this neighbor.</td>
</tr>
<tr>
<td>Message statistics</td>
<td>Statistics organized by message type.</td>
</tr>
<tr>
<td>InQ depth is</td>
<td>Number of messages in the input queue.</td>
</tr>
<tr>
<td>OutQ depth is</td>
<td>Number of messages in the output queue.</td>
</tr>
<tr>
<td>Sent</td>
<td>Total number of transmitted messages.</td>
</tr>
<tr>
<td>Received</td>
<td>Total number of received messages.</td>
</tr>
<tr>
<td>Opens</td>
<td>Number of open messages sent and received.</td>
</tr>
<tr>
<td>notifications</td>
<td>Number of notification (error) messages sent and received.</td>
</tr>
<tr>
<td>Updates</td>
<td>Number of update messages sent and received.</td>
</tr>
<tr>
<td>Keepalives</td>
<td>Number of keepalive messages sent and received.</td>
</tr>
<tr>
<td>Route Refresh</td>
<td>Number of route refresh request messages sent and received.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of messages sent and received.</td>
</tr>
<tr>
<td>Default minimum time between...</td>
<td>Time, in seconds, between advertisement transmissions.</td>
</tr>
<tr>
<td>For address family:</td>
<td>Address family for which the following fields refer.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.</td>
</tr>
<tr>
<td>neighbor version</td>
<td>Number used by Cisco IOS to track prefixes that have been sent and those that need to be sent.</td>
</tr>
<tr>
<td>...update-group</td>
<td>Number of update-group member for this address family.</td>
</tr>
<tr>
<td>Prefix activity</td>
<td>Prefix statistics for this address family.</td>
</tr>
<tr>
<td>Prefixes current</td>
<td>Number of prefixes accepted for this address family.</td>
</tr>
<tr>
<td>Prefixes total</td>
<td>Total number of received prefixes.</td>
</tr>
<tr>
<td>Implicit Withdraw</td>
<td>Number of times that a prefix has been withdrawn and readvertised.</td>
</tr>
<tr>
<td>Explicit Withdraw</td>
<td>Number of times that prefix is withdrawn because it is no longer feasible.</td>
</tr>
<tr>
<td>Used as bestpath</td>
<td>Number of received prefixes installed as a best paths.</td>
</tr>
<tr>
<td>Used as multipath</td>
<td>Number of received prefixes installed as multipaths.</td>
</tr>
<tr>
<td>* Saved (soft-reconfig)</td>
<td>Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a non-zero value.</td>
</tr>
<tr>
<td>* History paths</td>
<td>This field is displayed only if the counter has a non-zero value.</td>
</tr>
<tr>
<td>* Invalid paths</td>
<td>Number of invalid paths. This field is displayed only if the counter has a non-zero value.</td>
</tr>
</tbody>
</table>
### Table 41  show ip bgp neighbors Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Policy Denied Prefixes</td>
<td>Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a non-zero value.</td>
</tr>
<tr>
<td>* route-map</td>
<td>Displays inbound and outbound route-map policy denials.</td>
</tr>
<tr>
<td>* filter-list</td>
<td>Displays inbound and outbound filter-list policy denials.</td>
</tr>
<tr>
<td>* prefix-list</td>
<td>Displays inbound and outbound prefix-list policy denials.</td>
</tr>
<tr>
<td>* Ext Community</td>
<td>Displays only outbound extended community policy denials.</td>
</tr>
<tr>
<td>* AS_PATH too long</td>
<td>Displays outbound AS-path length policy denials.</td>
</tr>
<tr>
<td>* AS_PATH loop</td>
<td>Displays outbound AS-path loop policy denials.</td>
</tr>
<tr>
<td>* AS_PATH confed info</td>
<td>Displays outbound confederation policy denials.</td>
</tr>
<tr>
<td>* AS_PATH contains AS 0</td>
<td>Displays outbound denials of AS 0.</td>
</tr>
<tr>
<td>* NEXT_HOP Martian</td>
<td>Displays outbound martian denials.</td>
</tr>
<tr>
<td>* NEXT_HOP non-local</td>
<td>Displays outbound non-local next-hop denials.</td>
</tr>
<tr>
<td>* NEXT_HOP is us</td>
<td>Displays outbound next-hop-self denials.</td>
</tr>
<tr>
<td>* CLUSTER_LIST loop</td>
<td>Displays outbound cluster-list loop denials.</td>
</tr>
<tr>
<td>* ORIGINATOR loop</td>
<td>Displays outbound denials of local originated routes.</td>
</tr>
<tr>
<td>* unsuppress-map</td>
<td>Displays inbound denials due to an unsuppress-map.</td>
</tr>
<tr>
<td>* advertise-map</td>
<td>Displays inbound denials due to an advertise-map.</td>
</tr>
<tr>
<td>* VPN Imported prefix</td>
<td>Displays inbound denials of VPN prefixes.</td>
</tr>
<tr>
<td>* Well-known Community</td>
<td>Displays inbound denials of well-known communities.</td>
</tr>
<tr>
<td>* SOO loop</td>
<td>Displays inbound denials due to site-of-origin.</td>
</tr>
<tr>
<td>* Bestpath from this peer</td>
<td>Displays inbound denials because the bestpath came from the local router.</td>
</tr>
<tr>
<td>* Suppressed due to dampening</td>
<td>Displays inbound denials because the neighbor or link is in a dampening state.</td>
</tr>
<tr>
<td>* Bestpath from iBGP peer</td>
<td>Deploys inbound denials because the bestpath came from an iBGP neighbor.</td>
</tr>
<tr>
<td>* Incorrect RIB for CE</td>
<td>Deploys inbound denials due to RIB errors for a CE router.</td>
</tr>
<tr>
<td>* BGP distribute-list</td>
<td>Deploys inbound denials due to a distribute list.</td>
</tr>
<tr>
<td>Number of NLRIs...</td>
<td>Number of network layer reachability attributes in updates.</td>
</tr>
<tr>
<td>Connections established</td>
<td>Number of times a TCP and BGP connection have been successfully established.</td>
</tr>
<tr>
<td>dropped</td>
<td>Number of times that a valid session has failed or been taken down.</td>
</tr>
<tr>
<td>Last reset</td>
<td>Time since this peering session was last reset. The reason for the reset is displayed on this line.</td>
</tr>
<tr>
<td>Connection state</td>
<td>Connection status of the BGP peer.</td>
</tr>
<tr>
<td>Connection is ECN Disabled</td>
<td>Explicit congestion notification status (enabled or disabled).</td>
</tr>
</tbody>
</table>
### Table 41  `show ip bgp neighbors` Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local host: 10.108.50.1, Local port: 179</td>
<td>IP address of the local BGP speaker. BGP port number 179.</td>
</tr>
<tr>
<td>Foreign host: 10.108.50.2, Foreign port: 42698</td>
<td>Neighbor address and BGP destination port number.</td>
</tr>
<tr>
<td>Enqueued packets for retransmit:</td>
<td>Packets queued for retransmission by TCP.</td>
</tr>
<tr>
<td>Event Timers:</td>
<td>TCP event timers. Counters are provided for starts and wakeups (expired timers).</td>
</tr>
<tr>
<td>Retrans:</td>
<td>Number of times a packet has been retransmitted.</td>
</tr>
<tr>
<td>TimeWait:</td>
<td>Time waiting for the retransmission timers to expire.</td>
</tr>
<tr>
<td>AckHold:</td>
<td>Acknowledgement hold timer.</td>
</tr>
<tr>
<td>SendWnd:</td>
<td>Transmission (send) window.</td>
</tr>
<tr>
<td>KeepAlive:</td>
<td>Number of keep alive packets.</td>
</tr>
<tr>
<td>GiveUp:</td>
<td>Number times a packet is dropped due to no acknowledgement.</td>
</tr>
<tr>
<td>PmtuAger:</td>
<td>Path MTU discovery timer.</td>
</tr>
<tr>
<td>DeadWait:</td>
<td>Expiration timer for dead segments.</td>
</tr>
<tr>
<td>iss:</td>
<td>Initial packet transmission sequence number.</td>
</tr>
<tr>
<td>snduna:</td>
<td>Last transmission sequence number that has not been acknowledged.</td>
</tr>
<tr>
<td>sndnxt:</td>
<td>Next packet sequence number to be transmitted.</td>
</tr>
<tr>
<td>sndwnd:</td>
<td>TCP window size of the remote neighbor.</td>
</tr>
<tr>
<td>irs:</td>
<td>Initial packet receive sequence number.</td>
</tr>
<tr>
<td>rcvnxt:</td>
<td>Last receive sequence number that has been locally acknowledged.</td>
</tr>
<tr>
<td>rcvwnd:</td>
<td>TCP window size of the local host.</td>
</tr>
<tr>
<td>delrcvwnd:</td>
<td>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.</td>
</tr>
<tr>
<td>SRTT:</td>
<td>A calculated smoothed round-trip timeout.</td>
</tr>
<tr>
<td>RTTO:</td>
<td>Round-trip timeout.</td>
</tr>
<tr>
<td>RTV:</td>
<td>Variance of the round-trip time.</td>
</tr>
<tr>
<td>KRTT:</td>
<td>New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.</td>
</tr>
<tr>
<td>minRTT:</td>
<td>Smallest recorded round-trip timeout (hard-wire value used for calculation).</td>
</tr>
<tr>
<td>maxRTT:</td>
<td>Largest recorded round-trip timeout.</td>
</tr>
<tr>
<td>ACK hold:</td>
<td>Time the local host will delay an acknowledgment to carry (piggyback) additional data.</td>
</tr>
</tbody>
</table>
**Table 41  show ip bgp neighbors Field Descriptions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Precedence value:</td>
<td>IP precedence of the BGP packets.</td>
</tr>
<tr>
<td>Datagrams</td>
<td>Number of update packets received from a neighbor.</td>
</tr>
<tr>
<td>Rcvd:</td>
<td>Number of received packets.</td>
</tr>
<tr>
<td>with data</td>
<td>Number of update packets sent with data.</td>
</tr>
<tr>
<td>total data bytes</td>
<td>Total received in bytes.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of update packets sent.</td>
</tr>
<tr>
<td>Second Congestion</td>
<td>Number of update packets with data sent.</td>
</tr>
<tr>
<td>Datagrams: Rcvd</td>
<td>Number of update packets received from a neighbor.</td>
</tr>
<tr>
<td>out of order:</td>
<td>Number of packets received out of sequence.</td>
</tr>
<tr>
<td>with data</td>
<td>Number of update packets received with data.</td>
</tr>
<tr>
<td>Last reset</td>
<td>Elapsed time since this peering session was last reset.</td>
</tr>
<tr>
<td>unread input bytes</td>
<td>Number of bytes of packets still to be processed.</td>
</tr>
<tr>
<td>retransmit</td>
<td>Number of packets retransmitted.</td>
</tr>
<tr>
<td>fastretransmit</td>
<td>A duplicate acknowledgement is retransmitted for an out of order segment before the retransmission timer expires.</td>
</tr>
<tr>
<td>partialack</td>
<td>Number of retransmissions for partial acknowledgements (transmissions before or without subsequent acknowledgements).</td>
</tr>
<tr>
<td>Second Congestion</td>
<td>Second retransmission due to congestion.</td>
</tr>
</tbody>
</table>

**show ip bgp neighbors advertised-routes example**

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
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

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*1110.0.0.0</td>
<td>172.16.232.179</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>*200.2.2.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
```

Table 42 describes the significant fields shown in the display.

**Table 42  show ip bgp neighbors advertised-routes Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the local BGP speaker.</td>
</tr>
</tbody>
</table>
**Table 42**  *show ip bgp neighbors advertised-routes Field Descriptions (continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status codes</td>
<td>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 and will not be advertised to BGP neighbors. h—The table entry does not contain the best path based on historical information. *—The table entry is valid. &gt;—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>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 Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, this is the value of the inter-autonomous system metric. This field is not used frequently.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the set local-preference route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
</tbody>
</table>

**show ip bgp neighbors paths**

The following is example output from the *show ip bgp neighbors* command entered with the *paths* keyword:

```
Router# show ip bgp neighbors 172.29.232.178 paths ^10

Address    Refcount Metric Path
0x60E577B0   2     40 10 ?
```

Table 43 describes the significant fields shown in the display.
**show ip bgp neighbors received prefix-filter**

The following example shows that a prefix-list the filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
Router# show ip bgp neighbor 192.168.20.72 received prefix-filter
```

Address family: IPv4 Unicast

ip prefix-list 192.168.20.72:1 entries
  seq 5 deny 10.0.0.0/8 le 32

Table 43 describes the significant fields shown in the display.

**Table 43  show ip bgp neighbors paths Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Internal address where the path is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Number of routes using that path.</td>
</tr>
<tr>
<td>Metric</td>
<td>Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system path for that route, followed by the origin code for that route.</td>
</tr>
</tbody>
</table>

**show ip bgp neighbors received prefix-filter**

The following example shows that a prefix-list the filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
Router# show ip bgp neighbor 192.168.20.72 received prefix-filter
```

Address family: IPv4 Unicast

ip prefix-list 192.168.20.72:1 entries
  seq 5 deny 10.0.0.0/8 le 32

Table 44 describes the significant fields shown in the display.

**Table 44  show ip bgp neighbors received prefix-filter Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address family:</td>
<td>Address family mode in which the prefix filter is received.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Prefix list sent from the specified neighbor.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 45 describes the significant fields shown in the display.

**Table 45  show ip bgp paths Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Internal address where the path is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Hash bucket where path is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Number of routes using that path.</td>
</tr>
<tr>
<td>Metric</td>
<td>The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td>
</tr>
<tr>
<td>Path</td>
<td>The autonomous system path for that route, followed by the origin code for that route.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>(Optional) Displays information about that specific peer group.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays a summary of the status of all the members of a peer group.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 quote-regexp

To display routes matching the autonomous system path “regular expression,” use the show ip bgp quote-regexp command in EXEC mode.

    show ip bgp quote-regexp regexp

Syntax Description

regexp       “Regular expression” to match the Border Gateway Protocol (BGP) autonomous system paths.

Note       The regular expression has to be an exact match.

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the show ip bgp quote-regexp command in EXEC mode:

Router# show ip bgp quote-regexp "^10_" | begin 24.40

*  24.40.0.0/20    10.10.10.10                            0 10 2548 1239 10643 i
*  24.40.16.0/20   10.10.10.10                            0 10 2548 6172 i
*  24.40.32.0/19   10.10.10.10                            0 10 2548 6172 i
*  24.41.0.0/19    10.10.10.10                            0 10 2548 3356 3703 ?
*  24.42.0.0/17    10.10.10.10                            0 10 2548 6172 i

Note

Although the columns in the above display are not labeled, see Table 46 for detailed information.

Table 46 describes the significant fields shown in the display from left to right.
## BGP Commands

### show ip bgp regexp
Displays routes matching the autonomous system path regular expression.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp regexp</td>
<td>Displays routes matching the autonomous system path regular expression.</td>
</tr>
</tbody>
</table>

### Table 46 show ip bgp Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status codes</td>
<td>Status of the table entry; for example, * in the above display. 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 history. *—The table entry is valid. &gt;—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session. r—The table entry failed to install in the routing table. S—The table entry is a stale route.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity; for example, 24.40.0.0/20 in the above display.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next system that is used when forwarding a packet to the destination network; for example, 10.10.10.10. in the above display. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, the value of the interautonomous system metric.; for example, 0 in the above display.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the <code>set local-preference</code> route-map configuration command; for example, 10 in the above display. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters; for example, 2548 in the above display.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network; for example, 1239 in the above display. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>Origin of the entry; for example, ? in the above display. 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 <code>network</code> 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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>regexp</code></td>
<td>Regular expression to match the BGP autonomous system paths.</td>
</tr>
</tbody>
</table>

Command Modes

`EXEC`

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 Border Gateway Protocol (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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>Support for the <code>neighbor maximum-prefix</code> command was added to the output.</td>
</tr>
</tbody>
</table>
| 12.2    | • The number of networks and paths displayed in the output was split out to two separate lines.  
  • A field was added to display multipath entries in the routing table. |

**Usage Guidelines**

The `show ip bgp summary` command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route. A path is a route to a given destination. By default, BGP will install only a single path for each destination. If multipath routes are configured, BGP will install a path entry for each multipath route, and only one multipath route will be marked as the bestpath.

BGP attribute and cache entries are displayed in individually and in combinations that affect the bestpath selection process. The fields for this output are displayed when the related BGP feature is configured or attribute is received. Memory usage is displayed in bytes.

**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 using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
2 multipath network entries and 4 multipath paths
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 using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs
```
Table 47 shows the significant fields shown in the display. Fields that are preceded by the asterisk character are not shown in the above output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP router identifier</td>
<td>In order of precedence and availability, the router identifier specified by the <code>bgp router-id</code> command, a loopback address, or the highest IP address.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Internal version number of BGP database.</td>
</tr>
<tr>
<td>main routing table version</td>
<td>Last version of BGP database that was injected into the main routing table.</td>
</tr>
<tr>
<td>...network entries</td>
<td>Number of unique prefix entries in the BGP database.</td>
</tr>
<tr>
<td>...using ... bytes of memory</td>
<td>Amount of memory, in bytes, that is consumed for the path, prefix, or attribute entry displayed on the same line.</td>
</tr>
<tr>
<td>...path entries using</td>
<td>Number of path entries in the BGP database. Only a single path entry will be installed for a given destination. If multipath routes are configured, a path entry will be installed for each multipath route.</td>
</tr>
<tr>
<td>...multipath network entries using</td>
<td>Number of multipath entries installed for a given destination.</td>
</tr>
<tr>
<td>* ...BGP path/bestpath attribute entries using</td>
<td>Number of unique BGP attribute combinations for which a path is selected as the bestpath.</td>
</tr>
<tr>
<td>* ...BGP rrinfo entries using</td>
<td>Number of unique ORIGINATOR and CLUSTER_LIST attribute combinations.</td>
</tr>
<tr>
<td>...BGP AS-PATH entries using</td>
<td>Number of unique AS_PATH entries.</td>
</tr>
<tr>
<td>...BGP community entries using</td>
<td>Number of unique BGP community attribute combinations.</td>
</tr>
<tr>
<td>* ...BGP extended community entries using</td>
<td>Number of unique extended community attribute combinations.</td>
</tr>
<tr>
<td>BGP route-map cache entries using</td>
<td>Number of BGP route-map match and set clause combinations. A value of 0 indicates that the route cache is empty.</td>
</tr>
<tr>
<td>...BGP filter-list cache entries using</td>
<td>Number of filter-list entries that match an AS-path access list permit or deny statements. A value of 0 indicates that the filter-list cache is empty.</td>
</tr>
<tr>
<td>...received paths for inbound soft reconfiguration</td>
<td>Number paths received and stored for inbound soft reconfiguration.</td>
</tr>
<tr>
<td>BGP using...</td>
<td>Total amount of memory, in bytes, used by the BGP process.</td>
</tr>
<tr>
<td>Dampening enabled...</td>
<td>Indicates that BGP dampening is enabled. The number of paths that carry an accumulated penalty and the number of dampened paths are displayed on this line.</td>
</tr>
<tr>
<td>BGP activity...</td>
<td>Displays the number of times that memory has been allocated or released for a path or prefix.</td>
</tr>
</tbody>
</table>
### Table 47  show ip bgp summary Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>V</td>
<td>BGP version number spoken to the neighbor.</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous system number.</td>
</tr>
<tr>
<td>MsgRcvd</td>
<td>Number of messages received from the neighbor.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>Number of messages sent to the neighbor.</td>
</tr>
<tr>
<td>TblVer</td>
<td>Last version of the BGP database that was sent to the neighbor.</td>
</tr>
<tr>
<td>InQ</td>
<td>Number of messages queued to be processed from the neighbor.</td>
</tr>
<tr>
<td>OutQ</td>
<td>Number of messages queued to be sent to the neighbor.</td>
</tr>
<tr>
<td>Up/Down</td>
<td>The length of time that the BGP session has been in the Established state,</td>
</tr>
<tr>
<td></td>
<td>or the current status if not in the Established state.</td>
</tr>
<tr>
<td>State/PfxRcd</td>
<td>Current state of the BGP session, and the number of prefixes that</td>
</tr>
<tr>
<td></td>
<td>have been received from a neighbor or peer group. When the maximum</td>
</tr>
<tr>
<td></td>
<td>number (as set by the <code>neighbor maximum-prefix</code> command) is reached, the</td>
</tr>
<tr>
<td></td>
<td>string “PfxRcd” appears in the entry, the neighbor is shut down, and the</td>
</tr>
<tr>
<td></td>
<td>connection is set to Idle.</td>
</tr>
<tr>
<td></td>
<td>An (Admin) entry with Idle status indicates that the connection has</td>
</tr>
<tr>
<td></td>
<td>been shut down using the <code>neighbor shutdown</code> command.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show route-map</code></td>
<td>Displays configured route maps.</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip prefix-list</td>
<td>Resets the hit count of the prefix list entries.</td>
</tr>
<tr>
<td>distribute-list in</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>distribute-list out</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates an entry in a prefix list.</td>
</tr>
<tr>
<td>ip prefix-list description</td>
<td>Adds a text description of a prefix list.</td>
</tr>
<tr>
<td><strong>match ip address</strong></td>
<td>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.</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>neighbor prefix-list</strong></td>
<td>Distributes BGP neighbor information as specified in a prefix list.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address-family ipv4</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>address-family vpnv4</code></td>
<td>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.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>keepalive</code></td>
<td>Frequency (in seconds) with which the Cisco IOS software sends <code>keepalive</code> messages to its peer. The default is 60 seconds.</td>
</tr>
<tr>
<td><code>holdtime</code></td>
<td>Interval (in seconds) after not receiving a <code>keepalive</code> message that the software declares a peer dead. The default is 180 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>keepalive</code>: 60 seconds</td>
<td></td>
</tr>
<tr>
<td><code>holdtime</code>: 180 seconds</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router configuration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following example changes the <code>keepalive</code> timer to 70 seconds and the <code>holdtime</code> timer to 210 seconds:</td>
<td></td>
</tr>
<tr>
<td><code>timers bgp 70 210</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear ip bgp peer-group</code></td>
<td>Removes all the members of a BGP peer group.</td>
<td></td>
</tr>
<tr>
<td><code>router bgp</code></td>
<td>Configures the BGP routing process.</td>
<td></td>
</tr>
<tr>
<td><code>show ip bgp</code></td>
<td>Displays entries in the BGP routing table.</td>
<td></td>
</tr>
</tbody>
</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 48 maps the previous commands to their replacements.

<table>
<thead>
<tr>
<th>Old Command</th>
<th>Replacement Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>distance mbgp</td>
<td>distance bgp</td>
</tr>
<tr>
<td>match nlri</td>
<td>address-family ipv4</td>
</tr>
<tr>
<td></td>
<td>address-family vpnv4</td>
</tr>
<tr>
<td>set nlri</td>
<td>address-family ipv4</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>address-family vpnv4</td>
</tr>
<tr>
<td>show ip mbgp</td>
<td>show ip bgp ipv4 multicast</td>
</tr>
<tr>
<td>show ip mbgp summary</td>
<td>show ip bgp ipv4 multicast summary</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>(Optional) Specifies IP Version 4 multicast address prefixes.</td>
</tr>
<tr>
<td>unicast</td>
<td>(Optional) Specifies IP Version 4 unicast address prefixes.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance to associate with subsequent IP Version 4 address family configuration mode commands.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>neighbor activate</td>
<td>Enables the exchange of information with a BGP neighboring router.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>unicast</code></td>
<td>(Optional) Specifies VPN Version 4 unicast address prefixes.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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)#
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>address-family ipv4</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>neighbor activate</td>
<td>Enables the exchange of information with a BGP neighboring router.</td>
</tr>
</tbody>
</table>
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
Multiprotocol BGP Extensions for IP Multicast Commands

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.1</td>
<td>The route-map keyword was added.</td>
</tr>
<tr>
<td>11.1(20)CC</td>
<td>This mbgp keyword was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>This mbgp keyword was added.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip dvmrp</code></td>
<td>Displays information on DVMRP packets received and sent.</td>
</tr>
<tr>
<td><code>ip dvmrp accept-filter</code></td>
<td>Configures an acceptance filter for incoming DVMRP reports.</td>
</tr>
</tbody>
</table>
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**


**Defaults**

This command is disabled by default.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.1(20)CC</td>
<td>The <code>rtp</code> keyword was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>The <code>rtp</code> keyword was added.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip mpacket</td>
<td>Displays the contents of the circular cache-header buffer.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>route-map map-name</th>
<th>(Optional) Name of the route map that contains various BGP attribute settings.</th>
</tr>
</thead>
</table>

### Defaults

DVMRP routes are not redistributed into multiprotocol BGP.

### Command Modes

- Address family configuration
- Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1(20)CC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>Address family configuration mode was added.</td>
</tr>
</tbody>
</table>

### 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
```
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 mbgp` command is replaced by the `show ip bgp ipv4 multicast` command. See the description of the `show ip bgp ipv4 multicast` command for more information.
show ip bgp ipv4 multicast

To display IP Version 4 multicast database-related information, use the show ip bgp ipv4 multicast 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 49 describes the significant fields shown in the display.

**Table 49  show ip bgp ipv4 multicast Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>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. &gt;—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>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.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, the value of the interautonomous system metric.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the set local-preference route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip rpf</td>
<td>Displays how IP multicast routing does RPF.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 50 describes the significant fields shown in the display.

**Table 50  show ip bgp ipv4 multicast summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>IP address of configured neighbor in the multicast routing table.</td>
</tr>
<tr>
<td>V</td>
<td>Version of multiprotocol BGP used.</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous system to which the neighbor belongs.</td>
</tr>
<tr>
<td>MsgRcvd</td>
<td>Number of messages received from the neighbor.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>Number of messages sent to the neighbor.</td>
</tr>
<tr>
<td>TblVer</td>
<td>Number of the table version, which is incremented each time the table changes.</td>
</tr>
<tr>
<td>InQ</td>
<td>Number of messages received in the input queue.</td>
</tr>
</tbody>
</table>
Table 50  show ip bgp ipv4 multicast summary Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OutQ</td>
<td>Number of messages ready to go in the output queue.</td>
</tr>
<tr>
<td>Up/Down</td>
<td>Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).</td>
</tr>
<tr>
<td>State/PfxRcd</td>
<td>State of the neighbor/number of routes received. If no state is indicated, the state is up.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip rpf</td>
<td>Displays how IP multicast routing does RPF.</td>
</tr>
</tbody>
</table>
Multiprotocol BGP Extensions for IP Multicast Commands

show ip bgp ipv4 multicast summary
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (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.

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td>key-chain</td>
<td>Enables authentication for routing protocols.</td>
</tr>
<tr>
<td>key-string (authentication)</td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td>send-lifetime</td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
<tr>
<td>show key chain</td>
<td>Displays authentication key information.</td>
</tr>
</tbody>
</table>
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`: (Optional) Number or name of a standard IP access list to be applied to incoming routing updates.
- `ip-extended-list`: (Optional) Number or name of an 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The `access-list-number</td>
</tr>
<tr>
<td>11.3</td>
<td>The `access-list-number</td>
</tr>
<tr>
<td></td>
<td>The <code>ip</code> keyword was removed.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>ip-standard-list</code> and <code>ip-extended-list</code> arguments were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Table 51 lists default administrative distances.

```
Table 51  Default Administrative Distances

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route</td>
<td>1</td>
</tr>
<tr>
<td>Enhanced Interior Gateway Routing Protocol (EIGRP) summary route</td>
<td>5</td>
</tr>
<tr>
<td>External Border Gateway Protocol (eBGP)</td>
<td>20</td>
</tr>
<tr>
<td>Internal EIGRP</td>
<td>90</td>
</tr>
<tr>
<td>IGRP</td>
<td>100</td>
</tr>
<tr>
<td>Open Shortest Path First (OSPF)</td>
<td>110</td>
</tr>
<tr>
<td>Intermediate System-to-Intermediate System (IS-IS)</td>
<td>115</td>
</tr>
</tbody>
</table>
```
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>distance bgp</td>
<td>Allows the use of external, internal, and local administrative distances that could be a better route to a node.</td>
</tr>
</tbody>
</table>
## 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-number</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>access-list-name</code></td>
<td></td>
</tr>
<tr>
<td><code>in</code></td>
<td>Applies the access list to incoming routing updates.</td>
</tr>
<tr>
<td><code>interface-type</code></td>
<td>(Optional) Interface type.</td>
</tr>
<tr>
<td><code>interface-number</code></td>
<td>(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.</td>
</tr>
</tbody>
</table>

### Defaults

This command is disabled by default.

### Command Modes

Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-name</code>, <code>interface-type</code>, and <code>interface-number</code> arguments were added.</td>
</tr>
</tbody>
</table>

### 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 EIGRP 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 1
  network 10.108.0.0
  distribute-list 1 in
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>access-list (IP standard)</td>
<td>Defines a standard IP access list.</td>
</tr>
<tr>
<td>distribute-list out (IP)</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-number</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>access-list-name</code></td>
<td></td>
</tr>
<tr>
<td><code>out</code></td>
<td>Applies the access list to outgoing routing updates.</td>
</tr>
<tr>
<td><code>interface-name</code></td>
<td>(Optional) Name of a particular interface.</td>
</tr>
<tr>
<td><code>routing-process</code></td>
<td>(Optional) Name of a particular routing process, or the <code>static</code> or <code>connected</code> keyword.</td>
</tr>
<tr>
<td><code>as-number</code></td>
<td>(Optional) Autonomous system number.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <code>access-list-name</code> argument was added.</td>
</tr>
</tbody>
</table>

**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.
IP Routing Protocol-Independent Commands

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>access-list (IP standard)</td>
<td>Defines a standard IP access list.</td>
</tr>
<tr>
<td>distribute-list in (IP)</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>network-number</th>
<th>Number of the network.</th>
</tr>
</thead>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show ip route</td>
<td>Displays the current state of the routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match length</td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set default interface</td>
<td>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.</td>
</tr>
<tr>
<td>set interface</td>
<td>Indicates where to output packets that pass a match clause of route map for policy routing.</td>
</tr>
<tr>
<td>set ip default next-hop</td>
<td>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.</td>
</tr>
<tr>
<td>verify-availability</td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td>set ip next-hop</td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td>show ip local policy</td>
<td>Displays the route map used for local policy routing.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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, based on the destination IP address of the packet. 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>match ip address</strong></td>
<td>Distributes any routes that have a destination network number address that</td>
</tr>
<tr>
<td></td>
<td>is permitted by a standard or extended access list, and performs policy</td>
</tr>
<tr>
<td></td>
<td>routing on packets.</td>
</tr>
<tr>
<td><strong>match length</strong></td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td><strong>route-map (IP)</strong></td>
<td>Defines the conditions for redistributing routes from one routing protocol</td>
</tr>
<tr>
<td></td>
<td>into another, or enables policy routing.</td>
</tr>
<tr>
<td><strong>set default interface</strong></td>
<td>Indicates where to output packets that pass a match clause of a route map</td>
</tr>
<tr>
<td></td>
<td>for policy routing and have no explicit route to the destination.</td>
</tr>
<tr>
<td><strong>set interface</strong></td>
<td>Indicates where to output packets that pass a match clause of route map for</td>
</tr>
<tr>
<td></td>
<td>policy routing.</td>
</tr>
<tr>
<td><strong>set ip default next-hop</strong></td>
<td>Indicates where to output packets that pass a match clause of a route map</td>
</tr>
<tr>
<td></td>
<td>for policy routing and for which the Cisco IOS software has no explicit route to</td>
</tr>
<tr>
<td></td>
<td>a destination.</td>
</tr>
<tr>
<td><strong>set ip next-hop</strong></td>
<td>Indicates where to output packets that pass a match clause of a route map</td>
</tr>
<tr>
<td></td>
<td>for policy routing.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix</td>
<td>IP route prefix for the destination.</td>
</tr>
<tr>
<td>mask</td>
<td>Prefix mask for the destination.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the next hop that can be used to reach that network.</td>
</tr>
<tr>
<td>interface-type</td>
<td>Network interface type.</td>
</tr>
<tr>
<td>interface-number</td>
<td>Interface number that the specified interface type represents.</td>
</tr>
<tr>
<td>distance</td>
<td>(Optional) An administrative distance.</td>
</tr>
<tr>
<td>name</td>
<td>(Optional) Applies a name to the specified route.</td>
</tr>
<tr>
<td>permanent</td>
<td>(Optional) Specifies that the route will not be removed, even if the interface shuts down.</td>
</tr>
<tr>
<td>tag tag</td>
<td>(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps.</td>
</tr>
</tbody>
</table>

**Defaults**

No static routes are established.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
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.

```
Examples

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
```
ip route profile

To enable IP routing table statistics collection, use the **ip route profile** command in global configuration mode. To disable collection of routing table statistics, use the **no** form of the command.

```
ip route profile
no ip route profile
```

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

**Defaults**
The time interval for each sample, or sampling interval, is a fixed value and is set at 5 seconds.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The **ip route profile** command helps you to monitor routing table fluctuations that can occur as the result of route flapping, network failure, or network restoration.

This command identifies route flapping over brief time intervals. The time interval for each sample, or sampling interval, is a fixed value and is set at 5 seconds.

Two sets of statistics are collected. The per-interval statistics are collected over a sampling interval, while the routing table change statistics are the result of aggregating the per-interval statistics. The per-interval statistics are collected as a single set of counters, with one counter tracking one event. All counters are initialized at the beginning of each sampling interval; counters are incremented as corresponding events occur anywhere in the routing table.

At the end of a sampling interval, the per-interval statistics for that sampling interval are integrated with the routing table change statistics collected from the previous sampling intervals. The counters holding the per-interval statistics are reset and the process repeats.

Routing table statistics are collected for the following events:

- **Forward-Path Change.** This statistic is the number of changes in the forwarding path, which is the accumulation of prefix-add, next-hop change, and pathcount change statistics.
- **Prefix-Add.** A new prefix was added to the routing table.
- **Next-Hop Change.** A prefix is not added or removed, but the next hop changes. This statistic is only seen with recursive routes that are installed in the routing table.
- **Pathcount Change.** The number of paths in the routing table has changed. This statistic is the result of an increase in the number of paths for an Interior Gateway Protocol (IGP) prefix in the routing table.
- **Prefix Refresh.** Standard routing table maintenance; the forwarding behavior is not changed.

Use the **show ip route profile** command to display the routing table change statistics.
Examples

The following example enables the collection of routing table statistics:

```
ip route profile
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip route profile</code></td>
<td>Displays routing table change statistics.</td>
</tr>
</tbody>
</table>
ip routing protocol purge interface

To enable routing protocols to purge their routes when an interface goes down, use the `ip routing protocol purge interface` command in global configuration mode. To disable this function, use the `no` form of this command.

```
ip routing protocol purge interface
no ip routing protocol purge interface
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

If this command is not executed and a link goes down, the less efficient Routing Information Base (RIB) process is automatically triggered to delete all prefixes from the RIB that have the next hop on this interface. When the process works through a large routing table, it can consume many CPU cycles and increase convergence time.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(25.03)S01</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(27)SV</td>
<td>This command was integrated into Cisco IOS Release 12.0(27)SV.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This command was integrated into Cisco IOS Release 12.2 (18)SXE.</td>
</tr>
<tr>
<td>12.2(23.01)S</td>
<td>This command was integrated into Cisco IOS Release 12.2 (23.01)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ip routing protocol purge interface` command enables routing protocols that are capable of responding to interface failures to delete dependent routes from the RIB when a link on a router goes down and the interface is removed from the routing table.

**Examples**

In the following example, the purge interface function is enabled for a routing protocol.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip routing protocol purge interface
Router(config)# end
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (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.

```conf
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime</td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td>key chain</td>
<td>Enables authentication for routing protocols.</td>
</tr>
<tr>
<td>key-string (authentication)</td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td>send-lifetime</td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
<tr>
<td>show key chain</td>
<td>Displays authentication key information.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (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.
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime</td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td>ip rip authentication key-chain</td>
<td>Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.</td>
</tr>
<tr>
<td>key</td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td>key-string (authentication)</td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td>send-lifetime</td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
<tr>
<td>show key chain</td>
<td>Displays authentication key information.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime</td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td>key</td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td>key chain</td>
<td>Enables authentication for routing protocols.</td>
</tr>
<tr>
<td>send-lifetime</td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
<tr>
<td>service password-encryption</td>
<td>Encrypts passwords.</td>
</tr>
<tr>
<td>show key chain</td>
<td>Displays authentication key information.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-type</td>
<td>Interface type.</td>
</tr>
<tr>
<td>interface-number</td>
<td>Interface number.</td>
</tr>
</tbody>
</table>

**Defaults**

No match interfaces are defined.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</table>
match ip address

To distribute any routes that have a destination network number address that is permitted by a standard access list, an extended access list, or a prefix 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-number... | access-list-name...] | access-list-name [access-list-number... | access-list-name] | prefix-list prefix-list-name [prefix-list-name...]}

no match ip address {access-list-number [access-list-number... | access-list-name...] | access-list-name [access-list-number... | access-list-name] | prefix-list prefix-list-name [prefix-list-name...]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-number...</code></td>
<td>Number of a standard or extended access list. It can be an integer from 1 to 199. The ellipsis indicates that multiple values can be entered.</td>
</tr>
<tr>
<td><code>access-list-name...</code></td>
<td>Name of a standard or extended access list. It can be an integer from 1 to 199. The ellipsis indicates that multiple values can be entered.</td>
</tr>
<tr>
<td><code>prefix-list</code></td>
<td>Distributes routes based on a prefix list.</td>
</tr>
<tr>
<td><code>prefix-list-name...</code></td>
<td>Name of a specific prefix list. The ellipsis indicates that multiple values can be entered.</td>
</tr>
</tbody>
</table>

**Defaults**

No access list numbers or prefix lists are specified.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the `access-list-number`, `access-list-name`, or `prefix-list-name` arguments.

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 sections that contain specific `match` clauses. 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
```

Route maps that use prefix lists can be used for route filtering, default origination, and redistribution in other routing protocols. In the following example, a default route 0.0.0.0/0 is conditionally originated when there exists a prefix 10.1.1.0/24 in the routing table:

```
ip prefix-list cond permit 10.1.1.0/24
! route-map default-condition permit 10
  match ip address prefix-list cond
! router rip
default-information originate route-map default-condition
!```

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
!
routemap chicago
match ip address 6 25
set interface ethernet 0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip local policy route-map</td>
<td>Identifies a route map to use for policy routing on an interface.</td>
</tr>
<tr>
<td>ip policy route-map</td>
<td>Identifies a route map to use for policy routing on an interface.</td>
</tr>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match length</td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set default interface</td>
<td>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.</td>
</tr>
<tr>
<td>set interface</td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td>set ip default next-hop</td>
<td>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.</td>
</tr>
<tr>
<td>set ip next-hop</td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-number</td>
<td>Number or name of a standard or extended access list. It can be an integer from 1 to 199.</td>
</tr>
<tr>
<td>access-list-name</td>
<td></td>
</tr>
</tbody>
</table>

### Defaults

Routes are distributed freely, without being required to match a next hop address.

### Command Modes

Route-map configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>match as-path</strong></td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td><strong>match community-list</strong></td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td><strong>match interface (IP)</strong></td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td><strong>match ip address</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>match ip route-source</strong></td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td><strong>match metric (IP)</strong></td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td><strong>match route-type (IP)</strong></td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td><strong>match tag</strong></td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td><strong>route-map (IP)</strong></td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td><strong>set as-path</strong></td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td><strong>set automatic-tag</strong></td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td><strong>set community</strong></td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td><strong>set level (IP)</strong></td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td><strong>set local-preference</strong></td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td><strong>set metric (BGP, OSPF, RIP)</strong></td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td><strong>set metric-type</strong></td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td><strong>set next-hop</strong></td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td><strong>set tag (IP)</strong></td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td><strong>set weight</strong></td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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 | Number or name of a standard or extended access list. It can be an integer from 1 to 199. |
| access-list-name   |                                                                                           |

**Defaults**

No filtering on route source.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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** 10.0
- **Modification** 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip policy route-map</td>
<td>Identifies a route map to use for policy routing on an interface.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set default interface</td>
<td>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.</td>
</tr>
<tr>
<td>set interface</td>
<td>Indicates where to output packets that pass a match clause of route map for policy routing.</td>
</tr>
<tr>
<td>set ip default next-hop</td>
<td>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.</td>
</tr>
<tr>
<td>verify-availability</td>
<td></td>
</tr>
<tr>
<td>set ip next-hop</td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric-value</td>
<td>Route metric, which can be an IGRP five-part metric. It is a metric value from 0 to 4294967295.</td>
</tr>
</tbody>
</table>

### Defaults

No filtering on a metric value.

### Command Modes

Route-map configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributions any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributions routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributions routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributions routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Locally generated Border Gateway Protocol (BGP) routes.</td>
</tr>
<tr>
<td>internal</td>
<td>Open Shortest Path First (OSPF) intra-area and interarea routes or Enhanced Interior Gateway Routing Protocol (EIGRP) internal routes.</td>
</tr>
<tr>
<td>external [type-1</td>
<td>type-2]</td>
</tr>
<tr>
<td>level-1</td>
<td>Intermediate System-to-Intermediate System (IS-IS) Level 1 routes.</td>
</tr>
<tr>
<td>level-2</td>
<td>IS-IS Level 2 routes.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The local and external [type-1</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>number-paths</th>
<th>Maximum number of parallel routes an IP routing protocol installs in a routing table, in the range from 1 to 6.</th>
</tr>
</thead>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>(Optional) All interfaces become passive.</td>
</tr>
<tr>
<td><code>interface-type</code></td>
<td>Interface type.</td>
</tr>
<tr>
<td><code>interface-number</code></td>
<td>Interface number.</td>
</tr>
</tbody>
</table>

**Defaults**

Routing updates are sent on the interface.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0</td>
<td>The <code>default</code> keyword was added.</td>
</tr>
</tbody>
</table>

**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.

**Note**

For IS-IS you must keep at least one active interface and configure the interface with the `ip router isis` command.

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:

```plaintext
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):

```plaintext
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:

```plaintext
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 | transparent}] [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 | transparent}] [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`, `eigrp`, `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` or `eigrp` 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**: (Optional) 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.
**redistribute (IP)**

**Command Default**

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 1 | external 2**: 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 Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.

---

| **transparent** | (Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric. |
| **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. |
**Command Modes**

- Router configuration
- Address family configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>Address family configuration mode was added.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>Address family support under EIGRP was added in Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>Address family support under EIGRP was added in Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>Address family support under EIGRP was added.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**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 into OSPF from protocols other than OSPF or BGP, and no metric has been specified with the `metric-type` keyword and `type-value` argument, OSPF will use 20 as the default metric. When routes are redistributed into OSPF from BGP, OSPF will use 1 as the default metric. When routes are redistributed from one OSPF process to another OSPF process, Autonomous system (AS) external and not-so-stubby-area (NSSA) routes will use 20 as the default metric. When intra-area and inter-area routes are redistributed between OSPF processes, the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process. (This is the only case in which the routing table metric will be preserved when routes are redistributed into OSPF.)

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 shows how OSPF routes are redistributed into a BGP domain:

```plaintext
router bgp 109
   redistribute ospf
```

The following example causes Enhanced Interior Gateway Routing Protocol (EIGRP) routes to be redistributed into an OSPF domain:

```plaintext
router ospf 110
   redistribute eigrp
```

The following example causes the specified EIGRP process routes to be redistributed into an OSPF domain. The EIGRP-derived metric will be remapped to 100 and RIP routes to 200.

```plaintext
router ospf 109
   redistribute eigrp 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.

```plaintext
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):

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4 (BGP)</td>
<td>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.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>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.</td>
</tr>
<tr>
<td>default-information originate (BGP)</td>
<td>Allows the redistribution of network 0.0.0.0 into BGP.</td>
</tr>
<tr>
<td>default-information originate (IS-IS)</td>
<td>Generates a default route into an IS-IS routing domain.</td>
</tr>
<tr>
<td>default-information originate (OSPF)</td>
<td>Generates a default route into an OSPF routing domain.</td>
</tr>
<tr>
<td>distribute-list out (IP)</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>show route-map</td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip policy route-map</code></td>
<td>Identifies a route map to use for policy routing on an interface.</td>
</tr>
<tr>
<td><code>match as-path</code></td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td><code>match community-list</code></td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td><code>match interface (IP)</code></td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td><code>match ip address</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>match ip next-hop</code></td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td><code>match ip route-source</code></td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td><code>match length</code></td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td><code>match metric (IP)</code></td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td><code>match route-type (IP)</code></td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td><code>match tag</code></td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td><code>set as-path</code></td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td><code>set automatic-tag</code></td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td><code>set community</code></td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td><code>set default interface</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>set interface</code></td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td><code>set ip default next-hop</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>verify-availability</code></td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td><code>set ip next-hop</code></td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td><code>set level (IP)</code></td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td><code>set local-preference</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
<tr>
<td>show route-map</td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime</td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td>key</td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td>key chain</td>
<td>Enables authentication for routing protocols.</td>
</tr>
<tr>
<td>key-string (authentication)</td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td>show key chain</td>
<td>Displays authentication key information.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
<tr>
<td>show route-map</td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-type</td>
<td>Interface type, used with the interface number, to which packets are output.</td>
</tr>
<tr>
<td>interface-number</td>
<td>Interface number, used with the interface type, to which packets are output.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip policy route-map</td>
<td>Identifies a route map to use for policy routing on an interface.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match length</td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set interface</td>
<td>Indicates where to output packets that pass a match clause of route map for policy routing.</td>
</tr>
<tr>
<td>set ip default next-hop</td>
<td>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.</td>
</tr>
<tr>
<td>verify-availability</td>
<td></td>
</tr>
<tr>
<td>set ip next-hop</td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip policy route-map</code></td>
<td>Identifies a route map to use for policy routing on an interface.</td>
</tr>
<tr>
<td><code>match ip address</code></td>
<td>Distributes any routes that have a destination network number address that</td>
</tr>
<tr>
<td></td>
<td>is permitted by a standard or extended access list, and performs policy</td>
</tr>
<tr>
<td></td>
<td>routing on packets.</td>
</tr>
<tr>
<td><code>match length</code></td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td><code>route-map (IP)</code></td>
<td>Defines the conditions for redistributing routes from one routing protocol</td>
</tr>
<tr>
<td></td>
<td>into another, or enables policy routing.</td>
</tr>
<tr>
<td><code>set default interface</code></td>
<td>Indicates where to output packets that pass a match clause of a route map</td>
</tr>
<tr>
<td></td>
<td>for policy routing and have no explicit route to the destination.</td>
</tr>
<tr>
<td><code>set ip default next-hop</code></td>
<td>Indicates where to output packets that pass a match clause of a route map</td>
</tr>
<tr>
<td><code>verify-availability</code></td>
<td>for policy routing and for which the Cisco IOS software has no explicit route to a destination.</td>
</tr>
<tr>
<td><code>set ip next-hop</code></td>
<td>Indicates where to output packets that pass a match clause of a route map</td>
</tr>
<tr>
<td></td>
<td>for policy routing.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the next hop to which packets are output. The next hop must be an adjacent router.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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`
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.

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip policy route-map</code></td>
<td>Identifies a route map to use for policy routing on an interface.</td>
</tr>
<tr>
<td><code>match ip address</code></td>
<td>Distributes any routes that have a destination network number address that</td>
</tr>
<tr>
<td></td>
<td>is permitted by a standard or extended access list, and performs policy</td>
</tr>
<tr>
<td></td>
<td>routing on packets.</td>
</tr>
<tr>
<td><code>match length</code></td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td><code>route-map (IP)</code></td>
<td>Defines the conditions for redistributing routes from one routing protocol</td>
</tr>
<tr>
<td></td>
<td>into another, or enables policy routing.</td>
</tr>
<tr>
<td><code>set default interface</code></td>
<td>Indicates where to output packets that pass a match clause of a route map</td>
</tr>
<tr>
<td></td>
<td>for policy routing and have no explicit route to the destination.</td>
</tr>
<tr>
<td><code>set interface</code></td>
<td>Indicates where to output packets that pass a match clause of route map for</td>
</tr>
<tr>
<td></td>
<td>policy routing.</td>
</tr>
<tr>
<td><code>set ip next-hop</code></td>
<td>Indicates where to output packets that pass a match clause of a route map</td>
</tr>
<tr>
<td></td>
<td>for policy routing.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1.05)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set ip next-hop verify-availability</code></td>
<td>Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to those next hops.</td>
</tr>
<tr>
<td><code>set ip next-hop</code></td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the next hop to which packets are output. The next hop must be an adjacent router.</td>
</tr>
</tbody>
</table>

**Defaults**

This command is disabled by default.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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`
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:

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip policy route-map</td>
<td>Identifies a route map to use for policy routing on an interface.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match length</td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set default interface</td>
<td>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.</td>
</tr>
<tr>
<td>set interface</td>
<td>Indicates where to output packets that pass a match clause of route map for policy routing.</td>
</tr>
<tr>
<td>set ip default next-hop</td>
<td>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.</td>
</tr>
<tr>
<td>verify-availability</td>
<td></td>
</tr>
</tbody>
</table>
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.

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

**Defaults**
This command is disabled by default.

**Command Modes**
Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(3)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 Policy Routing with CEF. Policy routing is configured to verify that
next hop 50.0.0.8 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.

```
ip cef
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 50.0.0.8
set ip next-hop verify-availability
route-map test permit 20
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show route-map ipc</td>
<td>Displays counts of the one-way route map IPC messages sent from the RP to the VIP when NetFlow policy routing is configured.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>number</th>
<th>name</th>
<th>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:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>routine</td>
<td>Number Name</td>
</tr>
<tr>
<td>1</td>
<td>priority</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>immediate</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>flash</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>flash-override</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>critical</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>internet</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>network</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default behavior.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fair-queue (WFQ)</td>
<td>Enables WFQ for an interface.</td>
</tr>
<tr>
<td>ip policy route-map</td>
<td>Identifies a route map to use for policy routing on an interface.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
</tbody>
</table>
**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>Imports routes into a Level 1 area.</td>
</tr>
<tr>
<td>level-2</td>
<td>Imports routes into a Level 2 subdomain.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Imports routes into Level 1 and Level 2.</td>
</tr>
<tr>
<td>stub-area</td>
<td>Imports routes into an Open Shortest Path First (OSPF) not-so-stubby area (NSSA) area.</td>
</tr>
<tr>
<td>backbone</td>
<td>Imports routes into an OSPF backbone area.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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-1
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
<tr>
<td>show route-map</td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp default local-preference</td>
<td>Changes the default local preference value.</td>
</tr>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set origin (BGP)</td>
<td>Sets the BGP origin code.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
</tbody>
</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 Interior Gateway Routing Protocol (EIGRP).

**Defaults**

The dynamically learned metric value.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
<tr>
<td>show route-map</td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**Note**

This command is not supported for redistributing routes into Border Gateway Protocol (BGP).

**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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match as-path</td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match community-list</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>match interface (IP)</td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match ip next-hop</td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td>match ip route-source</td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td>match metric (IP)</td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td>match route-type (IP)</td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td>match tag</td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set as-path</td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set level (IP)</td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td>set local-preference</td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td>set metric (BGP, OSPF, RIP)</td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td>set next-hop</td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td>set tag (IP)</td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td>set weight</td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
<tr>
<td>show route-map</td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>next-hop</td>
<td>IP address of the next hop router.</td>
</tr>
</tbody>
</table>

**Defaults**

Default next hop address.

**Command Modes**

Route-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>match as-path</strong></td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td><strong>match community-list</strong></td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td><strong>match interface (IP)</strong></td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td><strong>match ip address</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>match ip next-hop</strong></td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td><strong>match ip route-source</strong></td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td><strong>match metric (IP)</strong></td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td><strong>match route-type (IP)</strong></td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td><strong>match tag</strong></td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td><strong>route-map (IP)</strong></td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td><strong>set as-path</strong></td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td><strong>set automatic-tag</strong></td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td><strong>set community</strong></td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td><strong>set level (IP)</strong></td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td><strong>set local-preference</strong></td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td><strong>set metric (BGP, OSPF, RIP)</strong></td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td><strong>set metric-type</strong></td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td><strong>set tag (IP)</strong></td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td><strong>set weight</strong></td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
<tr>
<td><strong>show route-map</strong></td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
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.

```plaintext
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:

```plaintext
route-map tag
set tag 5
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>match as-path</code></td>
<td>Matches a BGP autonomous system path access list.</td>
</tr>
<tr>
<td><code>match community-list</code></td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td><code>match interface (IP)</code></td>
<td>Distributes any routes that have their next hop out one of the interfaces specified.</td>
</tr>
<tr>
<td><code>match ip address</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>match ip next-hop</code></td>
<td>Redistributes any routes that have a next hop router address passed by one of the access lists specified.</td>
</tr>
<tr>
<td><code>match ip route-source</code></td>
<td>Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.</td>
</tr>
<tr>
<td><code>match metric (IP)</code></td>
<td>Redistributes routes with the metric specified.</td>
</tr>
<tr>
<td><code>match route-type (IP)</code></td>
<td>Redistributes routes of the specified type.</td>
</tr>
<tr>
<td><code>match tag</code></td>
<td>Redistributes routes in the routing table that match the specified tags.</td>
</tr>
<tr>
<td><code>route-map (IP)</code></td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td><code>set as-path</code></td>
<td>Modifies an autonomous system path for BGP routes.</td>
</tr>
<tr>
<td><code>set automatic-tag</code></td>
<td>Automatically computes the tag value.</td>
</tr>
<tr>
<td><code>set community</code></td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td><code>set level (IP)</code></td>
<td>Indicates where to import routes.</td>
</tr>
<tr>
<td><code>set local-preference</code></td>
<td>Specifies a preference value for the autonomous system path.</td>
</tr>
<tr>
<td><code>set metric (BGP, OSPF, RIP)</code></td>
<td>Sets the metric value for a routing protocol.</td>
</tr>
<tr>
<td><code>set metric-type</code></td>
<td>Sets the metric type for the destination routing protocol.</td>
</tr>
<tr>
<td><code>set next-hop</code></td>
<td>Specifies the address of the next hop.</td>
</tr>
<tr>
<td><code>set tag (IP)</code></td>
<td>Sets a tag value of the destination routing protocol.</td>
</tr>
<tr>
<td><code>set weight</code></td>
<td>Specifies the BGP weight for the routing table.</td>
</tr>
<tr>
<td><code>show route-map</code></td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
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 52 describes the significant fields shown in the display.

Table 52 show ip cache policy Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total adds</td>
<td>Number of times a cache entry was created.</td>
</tr>
<tr>
<td>total deletes</td>
<td>Number of times a cache entry or the entire cache was deleted.</td>
</tr>
<tr>
<td>Type</td>
<td>“NH” indicates the set ip next-hop command.</td>
</tr>
<tr>
<td></td>
<td>“Int” indicates the set interface command.</td>
</tr>
<tr>
<td>Routemap</td>
<td>Name of the route map that created the entry; in this example, george.</td>
</tr>
<tr>
<td>sequence</td>
<td>Route map sequence number.</td>
</tr>
<tr>
<td>Age</td>
<td>Age of the cache entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>Output interface type and number.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next hop.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip route-cache</td>
<td>Configures the router to export the flow cache entry to a workstation when a flow expires.</td>
</tr>
</tbody>
</table>
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 53 describes the significant fields shown in the display.

**Table 53  show ip local policy Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map equal</td>
<td>The name of the route map is equal.</td>
</tr>
<tr>
<td>permit</td>
<td>The route map contains permit statements.</td>
</tr>
<tr>
<td>sequence</td>
<td>The sequence number of the route map, which determines in what order it is processed among other route maps.</td>
</tr>
<tr>
<td>Match clauses:</td>
<td>Clauses in the route map that must be matched to satisfy the permit or deny action.</td>
</tr>
<tr>
<td>Set clauses:</td>
<td>Set clauses that will be put into place if the match clauses are met.</td>
</tr>
<tr>
<td>Policy routing matches:</td>
<td>Number of packets that meet the match clauses.</td>
</tr>
<tr>
<td>packets</td>
<td></td>
</tr>
<tr>
<td>bytes</td>
<td>Number of bytes in the packets that meet the match clauses.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip local policy route-map</td>
<td>Identifies a route map to use for local policy routing.</td>
</tr>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match length</td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set default interface</td>
<td>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.</td>
</tr>
<tr>
<td>set interface</td>
<td>Indicates where to output packets that pass a match clause of route map for policy routing.</td>
</tr>
<tr>
<td>set ip default next-hop</td>
<td>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.</td>
</tr>
<tr>
<td>verify-availability</td>
<td></td>
</tr>
<tr>
<td>set ip next-hop</td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
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 54 describes the significant fields shown in the display.

**Table 54  show ip policy Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map equal</td>
<td>The name of the route map is equal.</td>
</tr>
<tr>
<td>permit</td>
<td>The route map contains permit statements.</td>
</tr>
<tr>
<td>sequence</td>
<td>Sequence number of the route map, which determines in what order it is processed among other route maps.</td>
</tr>
</tbody>
</table>
Table 54  show ip policy Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match clauses:</td>
<td>Clauses in the route map that must be matched to satisfy the permit or deny action.</td>
</tr>
<tr>
<td>Set clauses:</td>
<td>Set clauses that will be put into place if the match clauses are met.</td>
</tr>
<tr>
<td>Policy routing matches:</td>
<td>Number of packets that meet the match clauses.</td>
</tr>
<tr>
<td>packets</td>
<td></td>
</tr>
<tr>
<td>bytes</td>
<td>Number of bytes in the packets that meet the match clauses.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match ip address</td>
<td>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.</td>
</tr>
<tr>
<td>match length</td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set default interface</td>
<td>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.</td>
</tr>
<tr>
<td>set interface</td>
<td>Indicates where to output packets that pass a match clause of route map for policy routing.</td>
</tr>
<tr>
<td>set ip default next-hop</td>
<td>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.</td>
</tr>
<tr>
<td>verify-availability</td>
<td></td>
</tr>
<tr>
<td>set ip next-hop</td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
</tbody>
</table>
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
  172.160.72.20 100 0:55:41
  172.160.72.22 100 0:55:41
  172.160.72.23 100 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):

<table>
<thead>
<tr>
<th>Address</th>
<th>FiltIn</th>
<th>FiltOut</th>
<th>DistIn</th>
<th>DistOut</th>
<th>Weight</th>
<th>RouteMap</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.108.211.17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>192.108.213.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>198.6.255.13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>172.160.72.18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>172.160.72.19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>172.160.84.17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Routing for Networks:
192.108.209.0
192.108.211.0
198.6.254.0

Routing Information Sources:

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Distance</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.160.72.19</td>
<td>20</td>
<td>0:05:28</td>
</tr>
</tbody>
</table>

Distance: external 20 internal 200 local 200

Table 55 describes the significant fields shown in the display.

### Table 55  show ip protocols Field Descriptions for IGRP Processes

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Protocol is “igrp 109”</td>
<td>Specifies the routing protocol used.</td>
</tr>
<tr>
<td>Sending updates every 90 seconds</td>
<td>Specifies the time between sending updates.</td>
</tr>
<tr>
<td>next due in 44 seconds</td>
<td>Precisely when the next update is due to be sent.</td>
</tr>
<tr>
<td>Invalid after 270 seconds</td>
<td>Specifies the value of the invalid parameter.</td>
</tr>
<tr>
<td>hold down for 280</td>
<td>Specifies the current value of the hold-down parameter.</td>
</tr>
<tr>
<td>flushed after 630</td>
<td>Specifies the time (in seconds) after which the individual routing information will be thrown (flushed) out.</td>
</tr>
<tr>
<td>Outgoing update ...</td>
<td>Specifies whether the outgoing filtering list has been set.</td>
</tr>
<tr>
<td>Incoming update ...</td>
<td>Specifies whether the incoming filtering list has been set.</td>
</tr>
<tr>
<td>Default networks</td>
<td>Specifies how these networks will be handled in both incoming and outgoing updates.</td>
</tr>
<tr>
<td>IGRP metric</td>
<td>Specifies the value of the K0-K5 metrics, and the maximum hop count.</td>
</tr>
<tr>
<td>Redistributing</td>
<td>Lists the protocol that is being redistributed.</td>
</tr>
<tr>
<td>Routing</td>
<td>Specifies the networks for which the routing process is currently injecting routes.</td>
</tr>
<tr>
<td>Routing Information Sources</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
<tr>
<td></td>
<td>• Administrative distance</td>
</tr>
<tr>
<td></td>
<td>• Time the last update was received from this source</td>
</tr>
</tbody>
</table>
The following is sample output from the `show ip protocols` command, showing EIGRP process 77:

```
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:

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Distance</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.180.81.28</td>
<td>90</td>
<td>0:02:36</td>
</tr>
<tr>
<td>172.180.80.28</td>
<td>90</td>
<td>0:03:04</td>
</tr>
<tr>
<td>172.180.80.31</td>
<td>90</td>
<td>0:03:04</td>
</tr>
</tbody>
</table>

Distance: internal 90 external 170
```

Table 56 describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Protocol is “eigrp 77”</td>
<td>Name and autonomous system number of the currently running routing protocol.</td>
</tr>
<tr>
<td>Outgoing update filter list for all interfaces...</td>
<td>Indicates whether a filter for outgoing routing updates has been specified with the <code>distribute-list out</code> command.</td>
</tr>
<tr>
<td>Incoming update filter list for all interfaces...</td>
<td>Indicates whether a filter for incoming routing updates has been specified with the <code>distribute-list in</code> command.</td>
</tr>
<tr>
<td>Redistributing: eigrp 77</td>
<td>Indicates whether route redistribution has been enabled with the <code>redistribute</code> command.</td>
</tr>
<tr>
<td>Automatic network summarization...</td>
<td>Indicates whether route summarization has been enabled with the <code>auto-summary</code> command.</td>
</tr>
<tr>
<td>Routing for Networks:</td>
<td>Networks for which the routing process is currently injecting routes.</td>
</tr>
<tr>
<td>Routing Information Sources:</td>
<td>Lists all the routing sources that the Cisco IOS software is using to build its routing table. The following is displayed for each source:</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
<tr>
<td></td>
<td>• Administrative distance</td>
</tr>
<tr>
<td></td>
<td>• Time the last update was received from this source</td>
</tr>
<tr>
<td>Distance: internal 90 external 170</td>
<td>Internal and external distances of the router. Internal distance is the degree of preference given to EIGRP internal routes. External distance is the degree of preference given to EIGRP external routes.</td>
</tr>
</tbody>
</table>
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
    Redistribution: 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
    Redistribution: 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 \texttt{show ip route} command in EXEC mode.

\texttt{show ip route ([ip-address [mask] [longer-prefixes]] | [protocol [process-id]] | [list access-list-number | access-list-name])}

\textbf{Syntax Description}

- \texttt{ip-address} (Optional) Address about which routing information should be displayed.
- \texttt{mask} (Optional) Argument for a subnet mask.
- \texttt{longer-prefixes} (Optional) Specifies that only routes matching the \texttt{ip-address} and \texttt{mask} pair should be displayed.
- \texttt{protocol} (Optional) Name of a routing protocol, or the keyword \texttt{connected}, \texttt{static}, or \texttt{summary}. If you specify a routing protocol, use one of the following keywords: \texttt{bgp}, \texttt{egp}, \texttt{eigrp}, \texttt{hello}, \texttt{igrp}, \texttt{isis}, \texttt{ospf}, and \texttt{rip}.
- \texttt{process-id} (Optional) Number used to identify a process of the specified protocol.
- \texttt{list} (Optional) The \texttt{list} keyword is required to filter output by an access list name or number.
- \texttt{access-list-name} (Optional) Filters the displayed output from the routing table based on the specified access list name.
- \texttt{access-list-number} (Optional) Filters the displayed output from the routing table based on the specified access list number.

\textbf{Command Modes}

EXEC

\textbf{Command History}

\begin{tabular}{|l|l|}
\hline
\textbf{Release} & \textbf{Modification} \\
\hline
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 \texttt{process-id} argument was added. \\
11.0 & The \texttt{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 \texttt{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. \\
\hline
\end{tabular}
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, la - 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 [200/128] 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 [200/128] via 10.119.254.244, 0:02:23, Ethernet2
    E    172.90.208.0 [200/128] via 10.119.254.244, 0:02:23, 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, la - 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 57 describes the significant fields shown in the displays.

### Table 57  *show ip route* Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 58 describes the significant fields shown when using the `show ip route` command with an IP address (previous displays).

**Table 58  show ip route with Address Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing entry for 10.119.0.0 (mask 255.255.0.0)</td>
<td>Network number and mask.</td>
</tr>
<tr>
<td>Known via ...</td>
<td>Indicates how the route was derived.</td>
</tr>
<tr>
<td>distance</td>
<td>Administrative distance of the information source.</td>
</tr>
<tr>
<td>Tag</td>
<td>Integer that is used to implement the route.</td>
</tr>
<tr>
<td>Redistributing via ...</td>
<td>Indicates the redistribution protocol.</td>
</tr>
<tr>
<td>Last update from 10.108.35.13 on ...</td>
<td>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.</td>
</tr>
<tr>
<td>0:00:58 ago</td>
<td>Specifies the last time the route was updated, in hours:minutes:seconds.</td>
</tr>
<tr>
<td>Routing Descriptor Blocks:</td>
<td>Displays the next hop IP address followed by the information source.</td>
</tr>
<tr>
<td>10.108.35.13, from 10.108.35.13, 0:00:58 ago</td>
<td>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.</td>
</tr>
<tr>
<td>from...via ...</td>
<td>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.</td>
</tr>
<tr>
<td>Route metric</td>
<td>This value is the best metric for this routing descriptor block.</td>
</tr>
<tr>
<td>traffic share count</td>
<td>Number of uses for this routing descriptor block.</td>
</tr>
<tr>
<td>Total delay</td>
<td>Total propagation delay (in microseconds).</td>
</tr>
<tr>
<td>minimum bandwidth</td>
<td>Minimum bandwidth encountered when sending data along this route.</td>
</tr>
<tr>
<td>Reliability 255/255</td>
<td>Likelihood of successful packet transmission expressed as a number from 0 to 255 (255 is 100 percent reliability).</td>
</tr>
<tr>
<td>minimum MTU</td>
<td>Smallest maximum transmission unit (MTU) along the path.</td>
</tr>
<tr>
<td>Loading 2/255</td>
<td>Effective bandwidth of the route in kbps/255 is saturation.</td>
</tr>
<tr>
<td>Hops</td>
<td>Number of hops to the destination or to the router where the route first enters IGRP.</td>
</tr>
</tbody>
</table>

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, la - 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
C 172.19.0.0 255.255.255.0 is subnetted, 1 subnets
  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 172.110.0.0 255.255.255.0 is directly connected, Ethernet0
```

Router#
show ip route profile

To display routing table change statistics, use the **show ip route profile** command in EXEC mode.

```
show ip route profile
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command in combination with the **ip route profile** global configuration command to validate the routing table change statistics.

**Examples**

The following example shows the frequency of routing table changes in a 5-second sampling interval. In this example, the Prefix add change occurred 22 times in one interval and 24 times in another interval. The output represents this with a Fwd-path change value of 2 and a Prefix add value of 2:

```
Router# show ip route profile
```

```
<table>
<thead>
<tr>
<th>Change/interval</th>
<th>Fwd-path change</th>
<th>Prefix add</th>
<th>Next-hop Change Change</th>
<th>Pathcount Change</th>
<th>Prefix refresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>87</td>
<td>87</td>
<td>89</td>
<td>89</td>
<td>89</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Table 59 describes the significant fields shown in the display.
Table 59  show ip route profile Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change/interval</td>
<td>Represents the frequency buckets. A Change/interval of 20 represents the bucket that is incremented when a particular event occurs 20 times in a sampling interval. It is very common to see high counters for the Change/interval bucket for 0. This counter represents the number of sampling intervals in which there were no changes to the routing table. Route removals are not counted in the statistics, only route additions.</td>
</tr>
<tr>
<td>Fwd-path change</td>
<td>Number of changes in the forwarding path. This value represents the accumulation of Prefix add, Nexthop change, and Pathcount change.</td>
</tr>
<tr>
<td>Prefix add</td>
<td>A new prefix was added to the routing table.</td>
</tr>
<tr>
<td>Nexthop change</td>
<td>A prefix is not added or removed, but the next hop changes. This statistic is only seen with recursive routes that are installed in the routing table.</td>
</tr>
<tr>
<td>Pathcount change</td>
<td>The number of paths in the routing table has changed. This change is the result of an increase in the number of paths for an Interior Gateway Protocol (IGP).</td>
</tr>
<tr>
<td>Prefix refresh</td>
<td>Indicates standard routing table maintenance. The forwarding behavior was not changed.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip route profile</td>
<td>Enables IP routing table statistics collection</td>
</tr>
</tbody>
</table>
IP Routing Protocol-Independent Commands

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 60 describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Source</td>
<td>Routing protocol name, or the <code>connected</code>, <code>static</code>, or <code>internal</code> keyword.</td>
</tr>
<tr>
<td>Networks</td>
<td>Number of prefixes that are present in the routing table for each route source.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Number of subnets that are present in the routing table for each route source, including host routes.</td>
</tr>
<tr>
<td>Overhead</td>
<td>Any additional memory involved in allocating the routes for the particular route source other than the memory specified in the Memory field.</td>
</tr>
<tr>
<td>Memory</td>
<td>Number of bytes allocated to maintain all the routes for the particular route source.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip route</code></td>
<td>Displays the current state of the routing table.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 61 describes the significant fields shown in the display.

**Table 61  show ip route supernets-only Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>Border Gateway Protocol (BGP) derived, as shown in list of codes.</td>
</tr>
<tr>
<td>172.160.0.0 (mask is 255.255.0.0)</td>
<td>Supernet IP address.</td>
</tr>
<tr>
<td>[20/0]</td>
<td>Administrative distance (external/internal).</td>
</tr>
<tr>
<td>via 172.160.72.30</td>
<td>Next hop IP address.</td>
</tr>
<tr>
<td>0:00:50</td>
<td>Age of the route (how long ago the update was received).</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime</td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td>key</td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td>key chain</td>
<td>Enables authentication for routing protocols.</td>
</tr>
<tr>
<td>key-string (authentication)</td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td>send-lifetime</td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 62 describes the significant fields shown in the display.

**Table 62  show route-map Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>Name of the route map.</td>
</tr>
<tr>
<td>permit</td>
<td>Indicates that the route is redistributed as controlled by the set actions.</td>
</tr>
<tr>
<td>sequence</td>
<td>Number that indicates the position a new route map is to have in the list of route maps already configured with the same name.</td>
</tr>
<tr>
<td>Match clauses</td>
<td>Match criteria—conditions under which redistribution is allowed for the current route map.</td>
</tr>
<tr>
<td>tag</td>
<td>Set actions—the particular redistribution actions to perform if the criteria enforced by the <code>match</code> commands are met.</td>
</tr>
<tr>
<td>Set clauses</td>
<td>metric</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
</tbody>
</table>
**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.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(3)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 63 describes the significant fields shown in the first display.

**Table 63  `show route-map ipc` Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route-map RP IPC Config Updates Sent</td>
<td>IPC messages are being sent from the RP to the VIP.</td>
</tr>
<tr>
<td>Name:</td>
<td>Number of IPC messages sent about the name of the route map.</td>
</tr>
<tr>
<td>Match access-list:</td>
<td>Number of IPC messages sent about the access list.</td>
</tr>
<tr>
<td>Match length:</td>
<td>Number of IPC messages sent about the length to match.</td>
</tr>
<tr>
<td>Set precedence:</td>
<td>Number of IPC messages sent about the precedence.</td>
</tr>
<tr>
<td>Set tos:</td>
<td>Number of IPC messages sent about the type of service (ToS).</td>
</tr>
<tr>
<td>Set nexthop:</td>
<td>Number of IPC messages sent about the next hop.</td>
</tr>
<tr>
<td>Set interface:</td>
<td>Number of IPC messages sent about the interface.</td>
</tr>
<tr>
<td>Set default nexthop:</td>
<td>Number of IPC messages sent about the default next hop.</td>
</tr>
<tr>
<td>Set default interface:</td>
<td>Number of IPC messages sent about the default interface.</td>
</tr>
<tr>
<td>Clean all:</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set ip next-hop verify-availability</td>
<td>Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to that next hop.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.0(3)</td>
<td>This command became protocol independent when the <code>across-interfaces</code> keyword was added.</td>
</tr>
</tbody>
</table>

**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
```
Symbols

<cr> xvii
? command xvi

A
accept-lifetime command IP2R-474
access list filters, BGP IP2R-309, IP2R-346
address-family ipv4 command IP2R-454
address-family vpnv4 command IP2R-456
address ranges, summarizing
  IS-IS IP2R-146, IP2R-255
  OSPF IP2R-72
adjacency levels, IS-IS, specifying IP2R-204, IP2R-205
administrative distance
  BGP, setting IP2R-302
  defaults (table) IP2R-157, IP2R-476
  EIGRP, setting IP2R-157
  OSPF default IP2R-158, IP2R-476
  RIP default IP2R-158, IP2R-477
aggregate-address command IP2R-258
aggregate addresses, configuring for BGP IP2R-258
area authentication command IP2R-66
area default-cost command IP2R-68
area filter-list command IP2R-70
area nssa command IP2R-71
area-password command IP2R-196
area range command IP2R-72
area stub command IP2R-74
area virtual-link command IP2R-76
authentication
  MD5, RIP IP2R-497
  See also MD5 authentication
  auto-cost command IP2R-79
  autonomous systems
    BGP providing paths to remote networks IP2R-448
    boundary router IP2R-82, IP2R-523
    auto-summary (BGP) command IP2R-261
    auto-summary (Enhanced IGRP) command IP2R-152
    auto-summary (RIP) command IP2R-8

B
BGP
  community, matching IP2R-329
  extended community, matching IP2R-331
BGP (Border Gateway Protocol)
  administrative distance, setting IP2R-302
  aggregate address, configuring IP2R-258
  backdoor routes, indicating IP2R-387
  community attribute, sending to neighbor IP2R-372
  enabling IP2R-389
  extended community list, creating IP2R-318
  local preference value, setting IP2R-549
  metric type IP2R-402
  networks, specifying IP2R-385
  route dampening
    configuration factors IP2R-275
    dampening information, clearing IP2R-292
    enabling IP2R-275
    flap statistics, clearing IP2R-295
    suppressed routes, unsuppressing IP2R-292
  route filtering, access lists IP2R-309
Index

route filtering, neighbor filter-list command  IP2R-346
route map  IP2R-526
route reflector, configuring  IP2R-370
route reflectors, configuring  IP2R-269, IP2R-271
route summarization  IP2R-8, IP2R-152, IP2R-261
routing domain confederation  IP2R-272
sessions, resetting immediately  IP2R-282
soft reconfiguration  IP2R-269, IP2R-271
synchronization with IGPs  IP2R-448
TCP MD5 authentication  IP2R-355
timers, adjusting  IP2R-452
bgp always-compare-med command  IP2R-263
bgp bestpath as-path ignore command  IP2R-264
bgp bestpath compare-routerid  IP2R-265
bgp bestpath med confed command  IP2R-266
bgp bestpath missing-as-worst command  IP2R-268
bgp client-to-client reflection command  IP2R-269
bgp cluster-id command  IP2R-271
bgp confederation identifier command  IP2R-272
bgp confederation peers command  IP2R-274
bgp dampening command  IP2R-275
bgp default ipv4-unicast command  IP2R-277
bgp default local-preference command  IP2R-278
bgp deterministic med command  IP2R-279
bgp fast-external-fallover command  IP2R-282
bgp log-neighbor-changes command  IP2R-283
bgp maxas-limit command  IP2R-285
bgp redistribute-internal command  IP2R-286
bgp router-id command  IP2R-287
bgp rr-group command  IP2R-288
clear ip bgp dampening command  IP2R-292
clear ip bgp external command  IP2R-293
clear ip bgp flap-statistics command  IP2R-295
clear ip bgp peer-group command  IP2R-296
clear ip eigrp neighbors command  IP2R-153
clear ip ospf command  IP2R-80
clear ip peer-group command  IP2R-297
command modes, understanding  xv to xvi
commands
carriage return (<cr>)  xvii
cautions, usage in text  x
CEF (Cisco Express Forwarding) policy routing  IP2R-543
default form, using  xix
displaying (example)  xvii
default form, using  xix
compatible rfc 1583 command  IP2R-81
conditional default origination, IS-IS  IP2R-197
configurations, saving  xx
displaying (example)  xvii
default information (Enhanced IGRP) command  IP2R-154
default information originate (BGP) command  IP2R-298, IP2R-446
default information originate (IS-IS) command  IP2R-197
default information originate (OSPF) command  IP2R-82
default information originate (RIP) command  IP2R-9
default metric (BGP) command  IP2R-300
default metric (Enhanced IGRP) command  IP2R-155
default metric (IGRP) command  IP2R-42
default metric (OSPF) command  IP2R-84
default metric (RIP) command  IP2R-10
default networks, specifying  IP2R-483
default routes
default networks, specifying  IP2R-483
IP  IP2R-483
IP Enhanced IGRP  IP2R-154
IS-IS  IP2R-82, IP2R-197
OSPF  IP2R-82, IP2R-197
designated routers, IS-IS, specifying election  IP2R-219

distance bgp command  IP2R-302
distance command  IP2R-476
distance eigrp command  IP2R-157
distance mbgp command  
See distance bgp command
distance ospf command  IP2R-88
distribute-list in command  IP2R-304, IP2R-479
distribute-list in command (RIP, IGRP, EIGRP)  IP2R-11, IP2R-44, IP2R-159
distribute-list out command  IP2R-306, IP2R-481
distribute-list out command (RIP, IGRP, EIGRP)  IP2R-13, IP2R-46, IP2R-161
documentation
conventions ix
feedback, providing xi
modules  v to vii
online, accessing xi
ordering xi
Documentation CD-ROM xi
documents and resources, supporting viii
domain-password command  IP2R-199
domain-tag command  IP2R-90

E

EGP (Exterior Gateway Protocol) neighbor, relationships  IP2R-54
EIGRP (Enhanced IGRP)
administrative distance, setting  IP2R-157
authentication, enabling  IP2R-168
bandwidth  IP2R-170
disabling  IP2R-181
enabling  IP2R-181
filters
routes in updates  IP2R-479, IP2R-481
routing updates, preventing  IP2R-519
interfaces, displaying  IP2R-184
load balancing  IP2R-193

metric offset  IP2R-179
metrics, adjusting  IP2R-155
neighbor adjacency changes, logging  IP2R-163, IP2R-164, IP2R-165
offsets, applying  IP2R-33
redistribution, metrics for  IP2R-155
route authentication  IP2R-168
route feasibility, determining  IP2R-193
route redistribution  IP2R-155
route summarization  IP2R-8, IP2R-152, IP2R-261
split horizon, enabling  IP2R-173
timers, adjusting  IP2R-171, IP2R-172
timers active time  IP2R-191
traffic distribution, controlling  IP2R-192
eigrp log-neighbor-changes command  IP2R-163
eigrp log-neighbor-warnings command  IP2R-164
eigrp router-id command  IP2R-165
eigrp stub command  IP2R-166

F

Feature Navigator
See platforms, supported
filtering output, show and more commands xx
filters
EIGRP
routes in updates  IP2R-479, IP2R-481
routing updates, preventing  IP2R-519
IP, on sources of routing information  IP2R-476
flash updates
RIP
configuring the suppression of  IP2R-15
flash-update-threshold command  IP2R-15
Frame Relay, disabling split horizon  IP2R-25, IP2R-48

G

gateway of last resort, IGRP and RIP, computing  IP2R-483
global configuration mode, summary of xvi

H

hardware platforms
See platforms, supported
hello packets
EIGRP
  interval between IP2R-171
  valid time IP2R-172
IS-IS, setting interval IP2R-210
help command xvi
hold time, EIGRP IP2R-172

I

ignore lsa mospf command IP2R-92
IGRP (Interior Gateway Routing Protocol)
enabling IP2R-58
offsets
  applying IP2R-56
  routing metrics IP2R-56
traffic distribution, balancing IP2R-63
import map command IP2R-308
indexes, master viii
input-queue command IP2R-16
interface configuration mode, summary of xvi
interfaces, circuit type, IS-IS, specifying IP2R-204
IP
local policy routing, identifying the route map IP2R-485
multicast routing, packet headers, storing IP2R-461
policy routing
  enabling IP2R-527
  packet length, matching IP2R-510
  route map, identifying IP2R-487
precedence IP2R-545
redistribution, matching
  BGP autonomous system path access lists IP2R-327
  BGP community list IP2R-329, IP2R-331
  interfaces IP2R-501
  IP addresses IP2R-504
match criteria, route maps IP2R-527
metric of a route IP2R-512
next hop router addresses IP2R-506
route sources IP2R-508
route types IP2R-514
tags IP2R-516
redistribution, setting
  autonomous system path IP2R-390
  BGP origin code IP2R-404
  BGP weight IP2R-406
  community IP2R-394
  default interface IP2R-534
  default next hop IP2R-538
interface IP2R-536
level for importing routes IP2R-547
metric IP2R-551
metric type IP2R-553
next hop IP2R-400, IP2R-541, IP2R-555
preference for autonomous system IP2R-549
route maps IP2R-527
tag IP2R-396, IP2R-532
tag of destination routing protocol IP2R-557
redistribution, setting metric
  source IP address, validating IP2R-39
  source IP address, validating IP2R-39
  source IP address, validating IP2R-39
ip as-path access-list command IP2R-309
ip authentication key-chain eigrp command IP2R-168
ip authentication mode eigrp command IP2R-169
ip bandwidth-percent eigrp command IP2R-170
ip bgp-community new-format command IP2R-311
ip bgp fast-external-fallover command IP2R-313
ip community-list command IP2R-314
ip default-network command IP2R-483
ip dvmrp metric command IP2R-459
IP Enhanced IGRP
  default routes IP2R-154
  route redistribution IP2R-154
ip extcommunity-list command  IP2R-318
ip hello-interval eigrp command  IP2R-171
ip hold-time eigrp command  IP2R-172
ip local policy route-map command  IP2R-485
ip multicast cache-headers command  IP2R-461
ip ospf authentication command  IP2R-93
ip ospf authentication-key command  IP2R-94
ip ospf cost command  IP2R-95
ip ospf database-filter all out command  IP2R-97
ip ospf dead-interval command  IP2R-98
ip ospf demand-circuit command  IP2R-99
ip ospf flood-reduction command  IP2R-100
ip ospf hello-interval command  IP2R-101
ip ospf message-digest-key command  IP2R-102
ip ospf mtu-ignore command  IP2R-104
ip ospf name-lookup command  IP2R-105
ip ospf network command  IP2R-106
ip ospf priority command  IP2R-108
ip ospf retransmit-interval command  IP2R-109
ip ospf transmit-delay command  IP2R-110
ip policy route-map command  IP2R-487
ip prefix-list command  IP2R-321
ip prefix-list description command  IP2R-324
ip prefix-list sequence-number command  IP2R-326
ip rip authentication key-chain command  IP2R-17
ip rip authentication mode command  IP2R-18
ip rip receive version command  IP2R-19
ip rip send version command  IP2R-20
ip rip triggered command  IP2R-21
ip rip v2-broadcast command  IP2R-23
ip route command  IP2R-489
ip route profile command  IP2R-492
ip router isis command  IP2R-202
ip split-horizon (RIP) command  IP2R-25
ip split-horizon command  IP2R-48
ip split-horizon eigrp command  IP2R-173
ip summary-address eigrp command  IP2R-174
ip summary-address rip command  IP2R-27
IS-IS (Intermediate System-to-Intermediate System) adjacency, specifying  IP2R-204, IP2R-205
area passwords, configuring  IP2R-196
conditional default origination  IP2R-197
default route, generating  IP2R-82, IP2R-197
designated router election, specifying  IP2R-219
domain passwords, configuring  IP2R-199
enabling  IP2R-235
interface password, assigning  IP2R-218
link-state metrics, configuring  IP2R-217
LSP lifetime  IP2R-228
LSP refresh interval  IP2R-227
password authentication, configuring  IP2R-196
retransmission level, setting  IP2R-220
router support, specifying level  IP2R-223
isis circuit-type command  IP2R-204
isis csnp-interval command  IP2R-205
isis display delimiter (IS-IS) command  IP2R-206
isis display delimiter command  IP2R-206
isis hello-interval command  IP2R-210
isis hello-multiplier command  IP2R-212
isis hello-padding command  IP2R-200, IP2R-208
isis lsp-interval command  IP2R-214
isis mesh-group command  IP2R-215
isis metric command  IP2R-217
isis password command  IP2R-218
isis priority command  IP2R-219
isis retransmit-interval command  IP2R-220
isis retransmit-throttle-interval command  IP2R-222
is-type command  IP2R-223

K
key chain command  IP2R-497
key command  IP2R-495
key-string command  IP2R-499
link-state metrics, IS-IS, configuring  IP2R-217
load balancing, EIGRP  IP2R-193
local preference value, BGP, setting  IP2R-549
log-adj-changes command  IP2R-111
lsp-gen-interval command  IP2R-225
LSP lifetime (IS-IS)  IP2R-228
LSP refresh interval (IS-IS)  IP2R-227
lsp-refresh-interval (IS-IS) command  IP2R-227

match as-path command  IP2R-327
match community command  IP2R-329, IP2R-331, IP2R-399
match extcommunity command  IP2R-331
match interface command  IP2R-501
match ip address command  IP2R-503
match ip next-hop command  IP2R-506
match ip route-source command  IP2R-508
match length command  IP2R-510
match metric (IP) command  IP2R-512
match nri command
See address-family ipv4 command
match route-type (IP) command  IP2R-514
match tag command  IP2R-516
maximum-paths command  IP2R-333, IP2R-518
max-lsp-lifetime (IP) command  IP2R-228
max-meter router-lsa command  IP2R-119
MD5 (Message Digest 5) authentication
  EIGRP  IP2R-169
  OSPF  IP2R-66
  RIP  IP2R-497
TCP connections between BGP peers  IP2R-355
metric holddown command  IP2R-50
metric maximum-hops command  IP2R-51
metrics
  EIGRP, adjusting  IP2R-155
  redistribution, assigning  IP2R-10, IP2R-84
metric weights (Enhanced IGRP) command  IP2R-175
metric weights (IGRP) command  IP2R-52
MIB, descriptions online  viii
modes
See command modes, understanding
multi-interface load splitting, configuring  IP2R-583
multiprotocol BGP (Border Gateway Protocol), networks, specifying  IP2R-385

neighbor (EIGRP) command  IP2R-177
neighbor (IGRP) command  IP2R-54
neighbor (OSPF) command  IP2R-112
neighbor (RIP) command  IP2R-29
neighbor advertise-map command  IP2R-337
neighbor advertisement-interval command  IP2R-335
neighbor database-filter command  IP2R-114
neighbor default-originate command  IP2R-339
neighbor description command  IP2R-341
neighbor distribute-list command  IP2R-342
neighbor ebgp-multihop command  IP2R-345
neighbor filter-list command  IP2R-346
neighbor local-as command  IP2R-348
neighbor maximum-prefix command  IP2R-350
neighbor next-hop-self command  IP2R-352
neighbor password command  IP2R-355
neighbor peer-group command
  creating  IP2R-359
  members, assigning  IP2R-357
neighbor prefix-list command  IP2R-362
neighbor remote-as command  IP2R-364
neighbor remove-private-as command  IP2R-366
neighbor resets, enabling logging  IP2R-283
neighbor route-map command  IP2R-368
neighbor route-reflector-client command  IP2R-370
neighbor send-community command  IP2R-372
neighbor shutdown command  IP2R-374
neighbor soft-reconfiguration inbound command  IP2R-375
neighbor unsuppress-map command  IP2R-378
neighbor update-source command  IP2R-380
neighbor version command  IP2R-381
neighbor weight command  IP2R-383
net command  IP2R-229
NetFlow policy routing  IP2R-543, IP2R-544, IP2R-581
network (BGP and multiprotocol BGP) command  IP2R-385
network (Enhanced IGRP) command  IP2R-178
network (IGRP) command  IP2R-55
network (RIP) command  IP2R-30
network area command  IP2R-115
network backdoor command  IP2R-387
network weight command  IP2R-389
new information in this release  ix
notes, usage in text  x
NSSA (not-so-stubby area), configuring  IP2R-71

O

ODR (On-Demand Routing), enabling  IP2R-2
offset-list (Enhanced IGRP) command  IP2R-179
offset-list (IGRP) command  IP2R-56
offset-list (RIP) command  IP2R-31
offsets
  EIGRP  IP2R-179
  IGRP  IP2R-56
  RIP  IP2R-31, IP2R-33
OSPF (Open Shortest Path First)
  address range for a single route, specifying  IP2R-72
  aggregate addresses, creating  IP2R-146
  area ID  IP2R-115
  authentication for an area, enabling  IP2R-66
  authentication type  IP2R-93
  auto cost  IP2R-79
  consolidate routes at a boundary  IP2R-72
  cost  IP2R-95
  cost to the default external route, assigning  IP2R-68
database, displaying information  IP2R-124
dead interval  IP2R-98
default metrics  IP2R-79
default metric values, setting  IP2R-84
default route, generate  IP2R-82
default summary route cost  IP2R-68
demand circuit  IP2R-99
designated router  IP2R-108
distance  IP2R-88
DNS names  IP2R-105
  enabling  IP2R-119
  hello packet interval  IP2R-98, IP2R-101
  interface information, displaying  IP2R-137
  interfaces  IP2R-115
  link-state advertisement retransmissions  IP2R-109
  LSA group pacing  IP2R-148
  MD5 authentication  IP2R-102
  MOSPF packets, ignoring  IP2R-92
  neighbor information, displaying  IP2R-139
  neighbor state changes, viewing  IP2R-111
  network type  IP2R-106
  not-so-stubby area, configuring  IP2R-71
  packet pacing  IP2R-135
  password  IP2R-94
  priority of router  IP2R-108
  retransmit interval  IP2R-109
  RFC 1583 compatible  IP2R-81
  route calculation timers, configuring  IP2R-149
  router-id, enabling  IP2R-118
  routers interconnecting to nonbroadcast networks  IP2R-112
  routing processes, displaying information  IP2R-121
  routing table entries, displaying  IP2R-123
  stub area, defining  IP2R-74
  summarize routes at a boundary  IP2R-72
  timers  IP2R-149
  transmit delay  IP2R-110
  virtual link  IP2R-76
virtual links, displaying  IP2R-145
output-delay command  IP2R-33

partition avoidance command  IP2R-231
passive-interface command  IP2R-519
passwords
  IS-IS
    area, assigning on  IP2R-196
    authentication  IP2R-196
    domain, assigning on  IP2R-199
    interface, assigning on  IP2R-218
platforms, supported
  Feature Navigator, identify using  xxi
  release notes, identify using  xxi
policy routing
  based on address  IP2R-504
  based on packet length  IP2R-510
  CEF  IP2R-543
  enabling  IP2R-527
  local  IP2R-485
  local, route map, identifying  IP2R-485
  NetFlow  IP2R-543
  route map, identifying  IP2R-487
  to a default next hop  IP2R-538
  to a next hop  IP2R-400, IP2R-541
  to an interface  IP2R-536
  to default interface  IP2R-534
  prc-interval command  IP2R-233
privileged EXEC mode, summary of  xvi
prompts, system  xvi

R
redistribute (IP) command  IP2R-521
redistribute dvmrp command  IP2R-464
redistribute static ip command  IP2R-521
redistribution
  between routing domains  IP2R-521
  EIGRP
    metrics for  IP2R-155
    into other protocols  IP2R-526
  IP Enhanced IGRP
    of default routes  IP2R-154
    match criteria  IP2R-527
    match criteria, See also IP, redistribution route maps  IP2R-527
    routes, using same metric value  IP2R-84
    routing information  IP2R-394, IP2R-402, IP2R-404
    using route maps  IP2R-394, IP2R-402, IP2R-404
    See also IP, redistribution release notes
  redistribution, assigning metrics for  IP2R-10, IP2R-84
retransmission intervals, setting, IS-IS  IP2R-220
RFC
  full text, obtaining  viii
  RFC 1247
    authentication  IP2R-66
    poll interval  IP2R-112
  RFC 2370, opaque LSAs  IP2R-126
RIP
  flash updates
    configuring the suppression of  IP2R-15
  RIP (Routing Information Protocol)
  IP
    adjust input queue  IP2R-16
    administrative distance  IP2R-158, IP2R-477
    automatic summarization  IP2R-8, IP2R-152
    default metric values, setting  IP2R-10
    default network  IP2R-483
delay between packets in update  IP2R-33
enabling  IP2R-34
metric offset  IP2R-31
redistribution  IP2R-479, IP2R-481
triggered  IP2R-21
version, global  IP2R-40
version, interface basis, receiving  IP2R-19
version, interface basis, sending  IP2R-20

IP authentication  IP2R-497, IP2R-499
accept lifetime  IP2R-474, IP2R-495
clear text  IP2R-18
enabling  IP2R-17
key  IP2R-495
key chain  IP2R-497
key information, displaying  IP2R-578
key string  IP2R-499
MD5  IP2R-18
send lifetime  IP2R-530
Version 2 update packets
broadcast packets
  sending  IP2R-24
multicast packets
  sending  IP2R-23
RIP, IP authentication
ROM monitor mode, summary of  xvi
route-map (IP) command  IP2R-526
route maps, BGP, applying to incoming and outgoing routes  IP2R-368
router bgp command  IP2R-389
route reflectors  IP2R-370
route reflectors, bgp cluster-id command  IP2R-271
router eigrp command  IP2R-181
router-id command  IP2R-118
router igrp command  IP2R-58
router isis command  IP2R-235
router odr command  IP2R-2
router ospf command  IP2R-119
router reflectors, bgp client-to-client reflection command  IP2R-269
router rip command  IP2R-34

route summarization
  automatic  IP2R-8, IP2R-152, IP2R-261
  IS-IS addresses  IP2R-146, IP2R-255
  OSPF addresses  IP2R-72
routing tables, default network in IP  IP2R-483

S

security
  See access lists, IP
send-lifetime command  IP2R-530
set as-path command  IP2R-390
set-attached bit command  IP2R-238
set-attached-bit command  IP2R-238
set-attached-bit route-map command  IP2R-238
set automatic-tag command  IP2R-238, IP2R-532
set community command  IP2R-394
set dampening command  IP2R-396
set default interface command  IP2R-534
set extcommunity command  IP2R-398
set interface command  IP2R-536
set ip default next-hop command  IP2R-538, IP2R-540
set ip next-hop (BGP) command  IP2R-400
set ip next-hop command  IP2R-541
set ip next-hop verify-availability command  IP2R-543
set ip precedence command  IP2R-545
set level (IP) command  IP2R-547
set local-preference command  IP2R-549
set metric (Enhanced IGRP) command  IP2R-182
set metric (IGRP) command  IP2R-59
set metric command (BGP, OSPF, RIP)  IP2R-551
set metric-type command  IP2R-553
set metric-type internal command  IP2R-402
set next-hop command  IP2R-555
set nlri command
  See address-family ipv4 command; address-family vpng4 command
set origin (BGP) command  IP2R-404
set origin command  IP2R-557
set-overload-bit command  IP2R-240
set tag command  IP2R-557
set weight command  IP2R-406
show ip bgp cidr-only command  IP2R-413
show ip bgp command  IP2R-408
show ip bgp community command  IP2R-415
show ip bgp community-list command  IP2R-417
show ip bgp dampened-paths command  IP2R-419
show ip bgp filter-list command  IP2R-421
show ip bgp flap-statistics command  IP2R-423
show ip bgp inconsistent-as command  IP2R-425
show ip bgp ipv4 command  IP2R-426
show ip bgp ipv4 multicast command  IP2R-467
show ip bgp ipv4 multicast summary command  IP2R-470
show ip bgp neighbors command  IP2R-428
show ip bgp paths command  IP2R-437
show ip bgp peer-group command  IP2R-438
show ip bgp regexp command  IP2R-441
show ip bgp summary command  IP2R-442
show ip cache policy command  IP2R-559
show ip eigrp interfaces command  IP2R-184
show ip eigrp neighbors command  IP2R-186
show ip eigrp topology command  IP2R-188
show ip eigrp traffic command  IP2R-190
show ip extcommunity-list command  IP2R-445
show ip local policy command  IP2R-560
show ip mbgp command  IP2R-561
See show ip bgp ipv4 multicast command
show ip mbgp summary command  IP2R-562
See show ip bgp ipv4 multicast summary command
show ip ospf border-routers command  IP2R-123
show ip ospf command  IP2R-121
show ip ospf database command  IP2R-124
show ip ospf flood-list command  IP2R-135
show ip ospf interface command  IP2R-137
show ip ospf neighbor command  IP2R-139
show ip ospf request-list command  IP2R-142
show ip ospf retransmission-list command  IP2R-143
show ip ospf summary-address command  IP2R-144
show ip ospf virtual-links command  IP2R-145
show ip policy command  IP2R-562
show ip protocols command  IP2R-564
show ip rip database command  IP2R-35
show ip route command  IP2R-568
show ip route profile command  IP2R-574
show ip route summary command  IP2R-576
show ip route supernets-only command  IP2R-577
show isis database command  IP2R-242
show isis lsp-log  IP2R-246
show isis spf-log command  IP2R-248
show isis topology command  IP2R-251
show key chain command  IP2R-578
show route-map command  IP2R-579
show route-map ipc command  IP2R-581
SMDS (Switched Multimegabit Data Service), disabling  split horizon  IP2R-25, IP2R-48
soft reconfiguration  IP2R-375
spf-interval command  IP2R-253
split horizon, EIGRP  IP2R-173
static routes  configuring  IP2R-489
IP  establishing  IP2R-489
redistributing  IP2R-521
stub area, OSPF  IP2R-74
summary-address (IS-IS) command  IP2R-255
summary-address command  IP2R-146
summary addresses, EIGRP  IP2R-174
synchronization, definition  IP2R-448
synchronization command  IP2R-448
T
Tab key, command completion  xvi
TCP, enabling MD5 authentication, BGP  IP2R-355
timers  BGP, adjusting  IP2R-452
EIGRP, adjusting  IP2R-171, IP2R-172

timers active-time command  IP2R-191

timers basic command  IP2R-4, IP2R-37, IP2R-61

timers bgp command  IP2R-452

timers lsa-group-pacing command  IP2R-148

timers spf command  IP2R-149

traffic-share (IGRP) command  IP2R-63

traffic-share balanced (Enhanced IGRP) command  IP2R-192

traffic-share balanced (IGRP) command  IP2R-63

traffic-share min command  IP2R-583

U

user EXEC mode, summary of  xvi

V

validate-update-source command  IP2R-39

variance (Enhanced IGRP) command  IP2R-193

variance (IGRP) command  IP2R-64

version command  IP2R-40