Software Configuration Guide for Cisco IOS Release 15.3(4)T

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408-526-4000
800-553-NETS (6387)
Fax: 408-527-0883

Text Part Number:

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Software Configuration Guide for Cisco IOS Release 15.3(4)T

CONTENTS

Preface

This preface describes the audience, organization, and documentation conventions for this guide and provides information on how to obtain related documents and technical assistance.

This preface includes the following major sections:

Audience

This guide is also intended for system integrators incorporating the Cisco 5930 Embedded Services Router (ESR) and the Cisco 5921 ESR into their designs. This book documents the Cisco IOS.

Organization

This guide is organized into the following chapters:

Chapter	Title	Description
1	Product Overview	Introduces new features
2	Using the Command Line	Describes how to use the Command Line Interface (CLI)
3	Configuring the Interfaces	Describes configuring interfaces and verifying connectivity
4	IP Mobility	Introduces Cisco IP mobility

Chapter	Title	Description
5	Introduction to Radio Aware Routing and MANET	Provides an overview of the protocols supported for MANET.
6	Understanding and Configuring DLEP	Describes how to configure the Dynamic Link Exchange Protocol (DLEP).
7	Configuring R2CP	Describes how to configure the Router to Radio Control Protocol (R2CP). This feature is available on only the Cisco 5921 ESR.
8	Configuring PPPoE	Describes how to configure Point-to-Point Protocol over Ethernet (PPPoE).
9	OSPFv3 Address Families	Describes how to use OSPFv3 address families to route IPv6 packets over OSPFv3—using IPv4 or IPv6 addresses. This chapter also describes how to configure and use OSPFv3 address families in conjunction with MANETs and RAR.
10	Configuring OSPFv3 for a MANET	Describes how to configure OSPFv3 in a MANET.
11	Configuring EIGRP in a MANET	Describes how to configure the Enhanced Interior Gateway Routing Protocol (EIGRP) in a MANET.
12	Understanding and Configuring IP Multiplexing	Discusses IP multiplexing for satellite topologies.
13	Zeroization	Discusses erasing any and all potentially sensitive information in the router. his feature is available on only the Cisco 5930 ESR.
Appendix A	Command Reference	Describes the commands referenced in this book.
Appendix B	System Message Overview	Describes the system messages specific to Cisco IOS Release 15.2(4)GC.
Appendix C	Technical Support Reference	Provides information intended only for reference while working with a Cisco Support engineer.

Related Documentation

Documentation for Cisco IOS Release 15.4(3)T includes the following documents:

- *Release Notes for Cisco IOS Software Release 15.4(3)T*
  http://www.cisco.com/c/en/us/td/docs/solutions/GGSG-Engineering/15-4-3M/15-4-3M.html
- *IP Mobility: Mobile Networks Configuration Guide, Cisco IOS Release 15.2M&T*
  http://www.cisco.com/en/US/partner/docs/ios-xml/ios/mob_ip/configuration/15-2mt/mob-ip-15-2mt-book.html

- *Cisco 5921 ESR Integration Guide*
  http://www.cisco.com/en/US/docs/solutions/GGSG-Engineering/Cisco_5921/Cisco_5921_ESR_Integration.pdf
- *Installing Cisco IOS on the X-Pedite 5205*
  http://www.cisco.com/en/US/docs/solutions/GGSG-Engineering/15_2_3GC/Install/X-ES_Instructions.pdf

For all documentation related to the main release, Cisco IOS Release 15.2T, refer to the following URL: http://www.cisco.com/en/US/partner/products/ps11746/tsd_products_support_series_home.html

For instructions on entering ROM Monitor code (ROMMON), refer to the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/sys-image-mgmt/configuration/15-2mt/sysimgmgmt-rebooting.html#GUID-1CC6B514-7873-4B93-A4DE-8E5FE02A042E

Conventions

This document uses the following typographical conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Command arguments for which you supply values are in *italics*.
[ ]	Command elements in square brackets are optional.
{ x | y | z }	Alternative keywords in command lines are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string because the string will include the quotation marks.
`screen` font	System displays are in `screen` font.
`boldface screen` font	Information you must enter verbatim is in **`boldface screen`** font.
`italic screen` font	Arguments for which you supply values are in *`italic screen`* font.
⟶	This pointer highlights an important line of text in an example.
^	Represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters such as passwords are in angle brackets.

Notes use the following conventions:

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

Cautions use the following conventions:

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

Warnings use the following conventions:

Warning **Safety warnings appear throughout this publication in procedures that, if performed incorrectly, may cause harm to you or the equipment. A warning symbol precedes each warning statement.**

Commands in Task Tables

Commands listed in task tables show only the relevant information for completing the task and not all available options for the command. For a complete description of a command, see Appendix A, "Command Reference."

Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at the following URL:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Product Overview

This chapter provides the following major sections to introduce the new features supported in Cisco IOS Release 15.4(3)T:

Cisco Unified Survivable Remote Site Telephony (SRST)

Cisco Unified Survivable Remote Site Telephony offers:

- Business resiliency through redundant, localized call processing.
- Intelligent and automatic failover configuration without manual IT or telecom intervention.
- Cost-effective operations through a converged voice and data network.
- Centralized IP telephony configuration and management.
- Investment protection and simplified migration.

Detailed information about using SRST can be found at the following link:

http://www.cisco.com/c/en/us/products/unified-communications/unified-survivable-remote-site-telephony/index.html

Locator/ID Separation Protocol (LISP)

Locator/ID Separation Protocol (LISP) is routing architecture that provides new semantics for IP addressing. The current IP routing and addressing architecture uses a single numbering space, the IP address, to express two pieces of information:

- Device identity.
- The way the device attaches to the network.

The LISP routing architecture design separates the device identity, or endpoint identifier (EID), from its location, or routing locator (RLOC), into two different numbering spaces. Splitting EID and RLOC functions yields several advantages.

Simplify Routing Operations

LISP enables enterprises and service providers to:

- Simplify multi-homed routing
- Facilitate scalable any-to-any WAN connectivity
- Support data center virtual machine mobility

Improve Scalability and Support

LISP routing architecture also:

- Improves scalability of the routing system through greater aggregation of RLOCs
- Optimizes IP routing for both IPv4 and IPv6 hosts
- Reduces operational complexities

LISP can be gradually introduced into an existing IP network without affecting the network endpoints or hosts.

There are several sources that provide detailed information about LISP. See the following links:

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

http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/locator-id-separation-protocol-lisp/datasheet_c78-576698.html

http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/locator-id-separation-protocol-lisp/qa_c67-582925.html

The following major sections are features carried over that were introduced in Cisco IOS Release15.2(4)GC:

- Cisco Wide Area Application Services (WAAS) Express, page 1-2

The following major sections are features carried over that were introduced in Cisco IOS Release 15.2(3)GC:

- Temperature Monitoring, page 1-3
- Real Time Clock, page 1-4
- Zeroization, page 1-4
- License Management, page 1-4

Cisco Wide Area Application Services (WAAS) Express

This release includes the Cisco® Wide Area Application Services (WAAS) Express which offers bandwidth optimization and application acceleration capabilities. The hardware and software requirements are:

- WAAS appliance running WAAS software 5.0.1 or later
- WAAS Central Manager running WAAS software 5.0.1 or later

Table 1 Recommended Sizing

Platform	TCP Connections	WAN Capacity	DRAM Required
5915	30	1.54 Mbps	512 MB
5921	75	4 Mbps	1 GB
5930	75	4 Mbps	1GB
5940	75	4 Mbps	1GB

Use the following configuration guidelines to enable Waas Express:

- Enter the following command to turn Waas Express on the Wan interface:

```
waas enable
```

- Enter the following commands to enable full optimizations:

```
parameter-map type waas waas_global
tfo optimize full
```

- Enter the following commands to enable application accelerators:

```
parameter-map type waas waas_global
accelerator http-express
enable
accelerator cifs-express
enable
accelerator ssl-express
enable
```

Detailed information about using the WAAS Express can be found at the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/wan_waas/configuration/15-2mt/wan-cfg-waas-exp.html

Temperature Monitoring

The temperature monitoring allow you set configure low and high temperature alarms and view the router temperature information and history. This feature is supported on only the Cisco 5930 Embedded Services Router (ESR).

The following commands are supported on the Cisco 5930 ESR:

- **monitor environment temperature**
- **monitor environmental temperature**
- **show environment**
- **show environment temperature**

For more information on configuring environmental monitoring, refer to the following URL: http://www.cisco.com/en/US/docs/routers/connectedgrid/cgr2010/software/15_2_1_t/swcg/cgr2010_15_2_1_t_swcg.html#wp2015437

Real Time Clock

The real time clock commands provide calender information from the X-ES X-Pedite5205 board. This feature is supported on only the Cisco 5930 Embedded Services Router.

The following real time clock commands are supported on the Cisco 5930 ESR:

- **clock calender-valid**
- **clock read-calender**
- **calender set**
- **clock update-calender**
- **ntp update-calender**
- **show clock detail**
- **show calender**

For more information on the real time clock commands, refer to the following URL: http://www.cisco.com/en/US/partner/docs/ios/mcl/allreleasemcl/all_book.html

Zeroization

Zeroization shuts down all network interfaces and causes zeroization of the Cisco IOS configuration and object code files, including all IP addresses on the router contained in volatile memory. This feature is supported on only the Cisco 5930 Embedded Services Router.

The following zeroization commands are supported on the Cisco 5930 ESR:

- **service declassify** {**erase-flash** | **erase-nvram** | **erase-all** | **erase-default**} [**trigger GPIO** *pin-number*]
- **show declassify**

For more information on zeroization, see Chapter 13, “Zeroization.”

License Management

The Cisco 5921 ESR uses a virtual Unique Device Identifier (UDI) from the software that you input into the license registration tool on cisco.com to acquire a software license. The Cisco 5921 ESR uses a virtual UDI because it is not a hardware-based platform with a fixed UDI. You use the license management commands to determine the license needed, generate a UDI, acquire and activate a software license and verify that the license installed correctly.

The following license commands are available on the Cisco 5921 ESR:

- **license clear**
- **license install**
- **license udi generate**
- **show license**
- **show license file**
- **show license udi** [**history**]

- **show platform software license**

For more information on the Cisco 5921 ESR and it’s software licensing capabilities, refer to the *Cisco 5921 Embedded Services Router Integration Guide*.

CHAPTER 2

Using the Command Line

This chapter describes the Command Line Interface (CLI) you use to configure platforms utilizing Cisco IOS 15.2(4) GC. This chapter includes the following major sections:

- Accessing the CLI, page 2-1
- Performing Command Line Processing, page 2-1
- Performing History Substitution, page 2-2
- Understanding Cisco IOS Command Modes, page 2-2
- Getting a List of Commands and Syntax, page 2-4

Note Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Note The examples in this chapter are not platform specific.

Accessing the CLI

You can access the Cisco IOS CLI through the Gigabit Ethernet 0/0 interface using Secure Shell (SSh) or Telnet to establish a Virtual TeletYpe (VTY) session with the router.

After accessing the CLI on the router, the screen displays the following message:

```
Press Return for Console prompt

Router> enable
Password:< >
Router#
```

Performing Command Line Processing

Commands are not case-sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

You can scroll through the last 20 commands stored in the history buffer and enter or edit a command at the prompt. Table 2-1 lists the keyboard shortcuts for entering and editing commands.

Table 2-1 Keyboard Shortcuts

Keystrokes	Result
Press **Ctrl-B** or press the **Left Arrow** key[1]	Moves the cursor back one character.
Press **Ctrl-F** or press the **Right Arrow** key[1]	Moves the cursor forward one character.
Press **Ctrl-A**	Moves the cursor to the beginning of the command line.
Press **Ctrl-E**	Moves the cursor to the end of the command line.
Press **Esc-B**	Moves the cursor back one word.
Press **Esc-F**	Moves the cursor forward one word.

[1] The Arrow keys function only on ANSI-compatible terminals, such as VT100s.

Performing History Substitution

The history buffer stores the last 20 command lines you entered. History substitution enables you to access these command lines without retyping them. Table 2-2 lists the history substitution commands.

Table 2-2 History Substitution Commands

Command	Purpose
Ctrl-P or the **Up Arrow** key[1]	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall older commands successively.
Ctrl-N or the **Down Arrow** key[1]	Returns to more recent commands in the history buffer after commands have been recalled with **Ctrl-P** or the **Up Arrow** key. Repeat the key sequence to recall more recent commands.
`Router# show history`	Lists the last several commands you entered in EXEC mode.

[1] The Arrow keys function only on ANSI-compatible terminals such as VT100s.

Understanding Cisco IOS Command Modes

The Cisco IOS user interface has many different modes: user EXEC, privileged EXEC (enable), global configuration, interface, subinterface, and protocol-specific modes. The commands available to you are dependent on your current command mode. To get a list of the commands in a given mode, enter a question mark (?) at the system prompt. See the Getting a List of Commands and Syntax section for more information.

Note For complete information about Cisco IOS command modes, see the *Cisco IOS Configuration Fundamentals Configuration Guide* and the *Cisco IOS Configuration Fundamentals Command Reference* at the following URL:
http://www.cisco.com/en/US/partner/products/ps11746/prod_command_reference_list.html

Working with Frequently Used Command Modes

When you start a session, you begin in user mode, also called user EXEC mode. Only a small subset of commands are available in EXEC mode. To have access to all commands, you must enter privileged EXEC mode, also called enable mode. To access the privileged EXEC mode, you must enter a password. When you are in the privileged EXEC mode, you can enter any EXEC command or access global configuration mode. Most EXEC commands are one-time commands, such as **show** commands, which display the current configuration status, and **clear** commands, which reset counters or interfaces. The **EXEC** commands are not saved when the Cisco router is rebooted.

The configuration modes allow you to make changes to the running configuration. If you save the configuration, these commands are stored when you reboot the router. You must start in global configuration mode. From global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and a variety of protocol-specific modes.

Table 2-3 lists and describes frequently used Cisco IOS modes.

Table 2-3 Frequently Used Cisco IOS Command Modes

Mode	What You Use It For	How to Access	Prompt
User EXEC	To connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and display system information.	Log in.	`Router>`
Privileged EXEC (enable)	To set operating parameters. The privileged command set includes the commands in user EXEC mode, as well as the **configure** command. Use the **configure** command to access the other command modes.	From user EXEC mode, enter the **enable** command and the enable password (if a password has been configured).	`Router#`
Global configuration	To configure features that affect the system as a whole, such as the system time or router name.	From privileged EXEC mode, enter the **configure terminal** command.	`Router(config)#`
Interface configuration	To enable or modify the operation of a Gigabit Ethernet, Fast Ethernet, E1/T1, or smart serial interface with **interface** commands.	From global configuration mode, enter the **interface** *type location* command.	`Router(config-if)#`

The Cisco IOS command interpreter, called the EXEC, interprets and runs the commands you enter. You can abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh** and the **configure terminal** command to **config t**.

When you type **exit**, the router backs out one level. To exit configuration mode completely and return to privileged EXEC mode, press **Ctrl-Z**.

When you type **end**, the router returns to EXEC mode.

Using the “do” Command

EXEC-level commands, such as the **show** commands, are not listed on the same modes as the subcommand modes, such as SEU configuration. Use this command to execute EXEC commands (such as show, clear, and debug commands) while configuring your routing device. After the EXEC command is executed, the system will return to the configuration mode you were using.

To execute an EXEC-level command from global configuration mode or any configuration submode, use the **do** command in any configuration mode:

Command	Purpose
Router(config)#**do** *command*	Allows execution of an EXEC-level command from global configuration mode or any configuration submode.

Getting a List of Commands and Syntax

In any command mode, you can get a list of available commands by entering a question mark (?).

To obtain a list of commands that begin with a particular character sequence, enter those characters followed by the question mark (?). Do not include a space before the question mark. This form of help is called word help, because it completes a word for you.

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you have already entered.

```
Router# show cdp ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbor entries
  traffic    CDP statistics
  |          Output modifiers
  <cr>

Router#
```

CHAPTER 3

Configuring the Interfaces

This chapter provides the following major sections to describe how to configure and verify a router-to-modem interface.

- Using the Interface Command, page 3-1
- Configuring Interfaces, page 3-2
- Monitoring and Maintaining Interfaces, page 3-4

Note For complete command syntax and usage, see Appendix A, "Command Reference."

Using the Interface Command

The following general instructions apply to all interface-configuration processes:

Step 1 At the privileged EXEC prompt, enter the **configure terminal** command to enter global configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 2 In global configuration mode, enter the **interface** command. Identify the interface type and the number of the connector on the interface card. The following example shows how to select a fast Ethernet interface of 0:

```
Router(config)# interface fastEthernet 0/0
Router(config-if)#
```

Note You do not need to add a space between the interface type and interface number. For example, in the preceding line you can specify either **fastEthernet0/0** or **fastEthernet 0/0**.

Step 3 Interface numbers are assigned at the factory at the time of installation. Enter the **show interfaces** EXEC command to see a list of all interfaces installed on your router. A report is provided for each interface that your router supports, as shown in this display:

```
Router(config-if)# Ctrl-Z
Router# show interfaces
FastEthernet0/0 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 001f.ca0f.6508 (bia 001f.ca0f.6508)
  Description: OPERATIONS ACCESS - DO NOT CHANGE ADDRESS
  Internet address is 9.9.9.10/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 254/255, txload 1/255, rxload 6/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 18/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 2627000 bits/sec, 231 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     86251 packets input, 119155372 bytes
     Received 5158 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 1 throttles
     27 input errors, 0 CRC, 0 frame, 0 overrun, 27 ignored
     0 watchdog
     0 input packets with dribble condition detected
     35714 packets output, 3513886 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

Step 4 Follow each **interface** command with the interface-configuration commands your particular interface requires. The commands you enter define the protocols and applications that run on the interface. The commands are collected and applied to the **interface** command until you enter another **interface** command or press **Ctrl-Z** to exit interface configuration mode and return to privileged EXEC mode.

Step 5 You can use the **exit** command to exit interface configuration mode and return to global configuration mode.

Step 6 After you configure an interface, you can check the status of the interface by using the EXEC **show** commands listed in the "Monitoring and Maintaining Interfaces" section on page 3-4.

Configuring Interfaces

The following subsections describe interface configuration procedures:

- Configuring an IP Address, page 3-3
- Adding a Description for an Interface, page 3-3

Configuring an IP Address

To configure an IPv4 address and subnet mask on an interface, perform the following task:

	Command	Purpose
Step 1	`Router(config)# interface gigabitEthernet interface`	Specifies the interface to be configured.
Step 2	`Router(config-if)# ip address ip-addr mask`	Sets the IP address.

Example

The following example shows how to set the IPv4 address 10.108.1.27 with subnet mask 255.255.255.0 on interface gigabitEthernet 0/0:

```
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip address 10.108.1.27 255.255.255.0
```

Adding a Description for an Interface

You can add a description about an interface to help you remember its function. The description displays in the output of the following commands: **show configuration**, **show running-config**, and **show interfaces**.

To add a description for an interface, enter the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# description string`	Adds a description for an interface.

Examples

This example shows how to add the description *Operations* on `gigabitEthernet interface 0/0`:

```
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# description Operations
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# show interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 001f.ca0f.6508 (bia 001f.ca0f.6508)
  Description: OPERATIONS ACCESS - DO NOT CHANGE ADDRESS
  Internet address is 10.108.1.27/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
 reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, 1000BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/38054/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     3289500 packets input, 1652322462 bytes
     Received 18932 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 37924 throttles
     1933147 input errors, 0 CRC, 0 frame, 0 overrun, 1933147 ignored
     0 watchdog
     0 input packets with dribble condition detected
     133400 packets output, 13054277 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

Monitoring and Maintaining Interfaces

The following sections describe how to monitor and maintain the interfaces:

- Monitoring Interface and Controller Status, page 3-4
- Clearing and Resetting the Interface Counters, page 3-6

Monitoring Interface and Controller Status

The router contains commands that you can enter at the EXEC prompt to display information about the interface. The following table lists some of the interface monitoring commands. You can display the full list of **show** commands by entering the **show ?** command at the EXEC prompt. These commands are fully described in the *Interface Command Reference*.

To display information about the interface, enter any of the following commands in user EXEC mode:

Command	Purpose
Router#**show interfaces** [*type interface*]	Displays the status and configuration of a specific interface or all interfaces.
Router#**show running-config**	Displays the configuration currently running in RAM.
Router#**show protocols** [*type interface*]	Displays the global (system-wide) and interface-specific status of any configured protocol.
Router#**show version**	Displays the hardware configuration, software version, names and sources of configuration files, and boot images.

This example shows how to display information about fastEthernet interface 0/0:

```
Router# show interfaces fastEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 001f.ca0f.6508 (bia 001f.ca0f.6508)
  Description: OPERATIONS ACCESS - DO NOT CHANGE ADDRESS
  Internet address is 10.108.1.27/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, 1000BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:25, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/38054/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     3289517 packets input, 1652328854 bytes
     Received 18949 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 37924 throttles
     1933147 input errors, 0 CRC, 0 frame, 0 overrun, 1933147 ignored
     0 watchdog
     0 input packets with dribble condition detected
     133525 packets output, 13066527 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

Clearing and Resetting the Interface Counters

To clear the interface counters shown with the **show interfaces** command, enter the following command:

Command	Purpose
Router#clear counters {*type interface*}	Clears interface counters.

This example shows how to clear and reset the counters on Gigabit Ethernet interface 0/0:

```
Router#clear counters gigabitEthernet 0/0
Clear "show interface" counters on this interface [confirm] y
Router#
*Sep 30 08:42:55: %CLEAR-5-COUNTERS: Clear counter on interface gigabitEthernet0/0
by vty1 (171.69.115.10)
Router#
```

The **clear counters** command (without any arguments) clears all the current interface counters from all interfaces.

Note The **clear counters** command does not clear counters retrieved with SNMP; it clears only those counters displayed with the EXEC **show interfaces** command.

CHAPTER 4

IP Mobility

This chapter provides the following major sections to describe the Cisco Mobile Ad-hoc Network (MANET):

Introduction to the Cisco Mobile Ad-hoc Network

The Cisco solution for MANETs provides the following capabilities:

- Optimal route selection based on Layer 2 feedback from the radio network
- Faster convergence when nodes join and leave the network
- Efficient integration of point-to-point, directional radio topologies with multi-hop routing
- Flow-controlled communications between each radio and its partner router
- OSPFv3 MANET features
  - OSPFv3 MANET Per Node Overlapping Relays
  - OSPFv3 MANET Selective Peering
- OSPFv3 Address Families
- VMI NBMA-Mode Multicast
- Dynamic Link Exchange Protocol (DLEP)—DLEP is a Radio Aware Routing (RAR) protocol providing efficient routing over Radio Frequencies (RF). DLEP functionality includes the following features:
  - IP Multicast support across Broadcast Multi-Access (BMA)
  - DLEP server interaction with an existing MANET infrastructure
  - DLEP server interaction with an existing Virtual Multipoint Interface (VMI)
  - Supported interaction between DLEP (and/or the underlying MANET infrastructure) and capabilities such as Address Resolution Protocol (ARP) and Cisco IOS Timer Services (Chapter 6, “Understanding and Configuring DLEP.”)

- Mobile Ad-hoc Network (MANET)—Cisco MANETs for router-to-radio communications address the challenges faced when merging IP routing with mobile radio communications. For more information, see Chapter 5, "Introduction to Radio Aware Routing and MANET."
- Virtual Multipoint Interfaces (VMI)—VMI provides services that map outgoing packets to the appropriate Point-to-Point Protocol over Ethernet (PPPoE) sessions. The VMI also provides a broadcast service that emulates a set of point-to-point connections as a point-to-multipoint interface with broadcast ability. For more information, see Chapter 8, "Configuring PPPoE" and Chapter 5, "Introduction to Radio Aware Routing and MANET."
- Enhanced Interior Gateway Routing Protocol (EIGRP)—EIGRP integrates the capabilities of link-state protocols into distance-vector protocols. In addition to providing fast convergence, EIGRP is distinguished from other routing protocols by supporting variable-length subnet masks, partial updates, and multiple network layer protocols. For more information, see Chapter 11, "Configuring EIGRP in a MANET."

Effective Networking in a MANET

The following are benefits of effective networking in a MANET environment:

- Routers and radios can interoperate efficiently, and without impacting operation of the radio network
- Radio point-to-point and router point-to-multipoint paradigms can be rationalized
- Radios can report status to routers for each link and each neighbor
- Routers can use this information to optimize routing decisions

Routing Challenges for MANETs

MANETs enable users deployed in areas with no fixed communications infrastructure to access critical voice, video, and data services. For example, soldiers in the field can employ unified communications, multimedia applications, and real-time information dissemination to improve situational awareness and respond quickly to changing battlefield conditions. Disaster managers can use video conferences, database access, and collaborative tools to coordinate multi-agency responses within an Incident Command System (ICS) framework. For event planners and trade show managers, MANETs represent a cost-effective way to accommodate mobile end users on a short-term basis. MANETs set the stage for more timely information sharing and faster, more effective decision-making.

Highly Dynamic Routing Topologies

In a Cisco MANET environment, highly mobile nodes communicate with each other across bandwidth-constrained radio links. An individual node includes both a radio and a network router, with the two devices interconnected over an Ethernet. Since these nodes can rapidly join or leave the network, MANET routing topologies are highly dynamic. Fast convergence in a MANET is challenging because the state of a node can change well before the event is detected by the normal timing mechanisms of the routing protocol.

Radio link quality in MANETs can vary dramatically because it can be affected by a variety of factors such as noise, fading, interference, and power fluctuation. As a result, avoiding congestion and determining optimal routing paths also pose significant challenges for the router network.

Topology Databases

Finally, directional radios that operate on a narrow beam tend to model the network as a series of physical point-to-point connections with neighbor nodes. This point-to-point model does not translate gracefully to multi-hop, multipoint router environments, as it increases the size of each router's topology database and reduces routing efficiency.

Router-to-Radio Links

Through the router-to-radio link, a radio can inform the router immediately when a node joins or leaves, and this enables the router to recognize topology changes more quickly than if it had to rely on timers. The link-status notification from the radio enables the router to respond faster to network topology changes. The radio passes metric information regarding the quality of a link to the router, enabling the router to more intelligently decide on which link to use.

Link-status Signaling

With link-status signaling provided by the router-to-radio link, applications such as voice and video work better because outages caused by topology changes are reduced or eliminated. Sessions are more stable.

Link-Quality Reporting

The quality of a radio link has a direct impact on throughput. The Cisco IOS software implements DLEP, RFC5578, OSFPv3, and EIGRP such that the route cost to a neighbor is updated dynamically based on radio-reported metrics, thus allowing the best route to be selected within a given set of radio links.

Link-Quality Metrics

Each routing protocol receives raw, radio-link data and computes a composite quality metric per link. In computing these metrics, the router may consider the following factors:

- Maximum Data Rate (MDR) — theoretical MDR of radio link, in scaled bits per second (bps)
- Current Data Rate (CDR)—CDR achieved on the link, in scaled bps
- Latency—encountered transmission-delay packets, in milliseconds
- Resources—a percentage (0-100) indicating remaining resource availability (such as battery power)
- Relative Link Quality (RLQ)—a numeric value (0-100) representing relative quality, where 100 indicates the highest quality

Router metrics can be weighted during the configuration process to emphasize or de-emphasize particular characteristics. For example, if throughput is a particular concern, you can weight the *throughput* metric so that it is factored more heavily into the composite route cost. Similarly, a metric of no concern can be omitted from the composite calculation.

Dynamic Reporting

Link metrics change rapidly, which can result in a flood of trivial routing updates. In a worst-case scenario, the network churns while reacting to relentless, minor variations. To prevent such churn, the Cisco IOS software provides a tunable dampening mechanism, thereby allowing you to configure thresholds. Any change in metrics below a configured threshold is ignored.

When the routing protocol is OSPFv3 or EIGRP, the connection quality for a neighbor session is determined by characteristics of that interface. The routing protocol receives dynamic, raw, radio link characteristics and computes a composite metric that is used to reduce the effect of frequent routing changes.

Tunable Hysteresis

A tunable hysteresis mechanism allows you to adjust the threshold to the routing changes that occur when the router receives a signal that a new peer has been discovered, or that an existing peer is unreachable. The tunable metric is weighted and adjusted dynamically to account for the following characteristics:

- Current and Maximum Bandwidth
- Latency
- Resources
- Relative Link Quality (RLQ)

Individual weights can be deconfigured and all weights can be cleared so that the cost returns to the default value per interface type. Based on the routing changes, cost can be determined by the application of these metrics.

Neighbor Up/Down Signaling

MANETs are highly dynamic environments. Neighbors enter and exit radio range rapidly. Each time a node joins or leaves the network, routers must reconstruct the topology logically. Routing protocols typically track topology changes with the use of timer-driven “hello” messages or neighbor timeouts. MANETs, however, cannot rely on such mechanisms given unacceptably slow convergence.

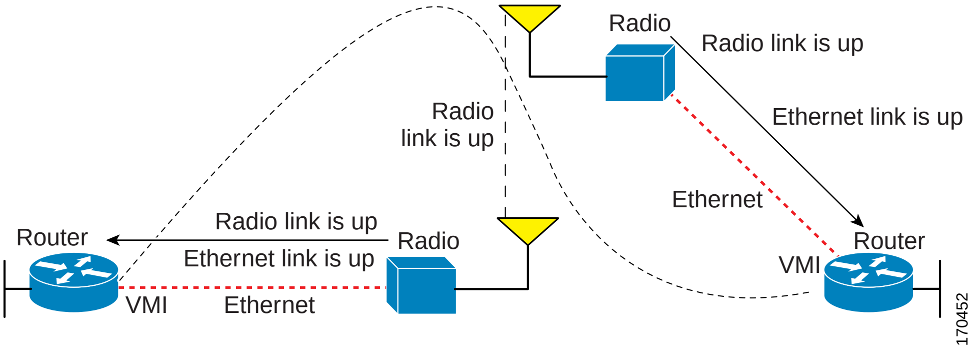
Neighbor Sessions

Each radio-router pair is a roaming client (or potential neighbor), constantly seeking new neighbors while checking for the continued existence of those already established. Neighbor discovery occurs when one radio discovers another. Each time a radio-to-radio link is established (between one neighbor and another), the radio initiates a neighbor session with its local router. When this neighbor session is successfully created and becomes active at both ends, router-to-router communication ensues—thereby completing the successful formation of a new neighbor session.

The neighbor up/down signaling capability in the Cisco IOS software provides faster network convergence by using link-status signals received from the local radio. The local radio notifies the router each time a link to a neighbor is established (up) or terminated (down), as depicted in Figure 4-1.

This change in link status occurs each time DLEP or RFC5578 creates or terminates a neighbor session.

Figure 4-1 Up and Down Signaling Sequence



OSPFv3 or EIGRP

The Cisco IOS routing protocol (OSPFv3 or EIGRP) responds immediately to each link-status signal by expediting a new adjacency (up—for a new neighbor) or tearing down an adjacency (down—for a neighbor suddenly lost). For example, if a vehicle drives behind a building and loses its connection, the router immediately senses the loss and establishes a new route to the vehicle through neighbors that are not blocked. This high-speed network convergence is essential for minimizing dropped voice calls and video disruptions.

When using VMI with RAR protocol and the link status changes (indicating a new or lost neighbor), the radio informs the router immediately of the topology change. Immediately upon receiving the link-status signal, the router declares the change and updates the routing tables.

Increased Performance

Link-status signaling provides the following benefits:

- Reduced routing delays
- Prevention of application time-outs
- Reliable and quick delivery of network-based applications and information over directional radio links
- Fast convergence and optimal route selection—preventing disruption of delay-sensitive traffic such as voice and video
- Reduced impact on radio equipment by minimizing the need for internal queuing/buffering
- Consistent Quality of Service (QoS) for multiple-radio networks
- Messaging enables dynamic rerouting to avoid disruptions and interference such as radio-link noise, fading, congestion, and power fade.

Dynamic Radio Capacities

The carrying capacity of each radio link may vary due to location changes or environmental conditions, and many radio-transmission systems have limited buffering capabilities. To minimize the need for packet queuing in the radio, the Cisco IOS software implements PPPoE with capabilities to control traffic buffering when congested.

Implementing flow-control also allows the use of fair queuing.

Credit-based Flow Control

The flow-control solution implements a credit-based mechanism documented in RFC 5578. When the PPPoE session is established, the radio can request a flow-controlled session. If the router acknowledges the request, all subsequent traffic must be flow-controlled. If a flow-control session has been requested and cannot be supported by the router, the session is terminated. Typically, both radio and router grant credits during session discovery. Once a device exhausts its credits, it must stop sending until additional credits have been granted. Credits can be added incrementally over the course of a session.

Metrics Scaling

High-performance radios use *metrics scaling* to meet high-speed link requirements. The radio can express the maximum and Current Data Rates (CDRs) with varying scalar values. Credit scaling allows a radio to change the default credit grant (or scaling factor) from 64 bytes to its default value.

You can use the **show vmi neighbor detail** command to display scalar values and maximum and current data rates (MDRs and CDRs).

CHAPTER 5

Introduction to Radio Aware Routing and MANET

After configuring the interfaces and verifying connectivity as described in Chapter 3, “Configuring the Interfaces,” you will need to configure each interface with the appropriate protocol.

This chapter provides the following major sections to describe Radio Aware Routing (RAR) for use in a Mobile Ad-hoc Network (MANET):

- Introduction to RAR, page 5-1
- MANET Protocols, page 5-2
- Understanding Virtual Templates, page 5-2
- Configuring QoS, page 5-3

Introduction to RAR

The Radio Aware Routing (RAR) strategy relies on a hierarchy of routing interfaces. At the top-most level is the Virtual Multipoint Interface, or VMI. The VMI provides a single, unified representation of the MANET to routing protocols (OSPFv3 or EIGRP), and to the rest of the attached topology.

For traffic originating outside the MANET, the VMI represents the ingress and egress point to and from the MANET. As traffic comes into the router, destined for the MANET, the router passes the traffic to the VMI interface. The VMI, in turn, fans the traffic out (based on destination) to the correct Virtual-Access interface, where QoS policy can be applied to queue the traffic based on the radio characteristics of the next hop. After applying (potentially different) QoS parameters on the Virtual-Access interfaces, the Virtual-Access interface funnels the traffic to the physical interface for transmission to the radio device.

The Virtual-Access interfaces are logically “underneath” the VMI interface. Each Virtual-Access interface represents a “destination” which is either a routing next-hop, or a multicast group. The QoS logic and associated queues on the Virtual-Access interfaces facilitate the fine-grained QoS. The Virtual-Access interface that exists for each next-hop or group gives the ability to vary QoS behavior on a hop-by-hop (or group-by-group) basis.

At the bottom of the interface hierarchy is the actual physical interface connecting the router and radio.

MANET Protocols

The protocols described in this guide support Mobile Ad-hoc Networks (MANETs). MANET-routing protocols provide signaling among MANET routers, including scope-limited flooding and point-to-point delivery of MANET routing protocol signaling in a multi-hop network. Packets may be unicast or multicast and use any appropriate transport protocol.

The RAR protocols supported Cisco IOS Release 15.2(1)GC provide the capabilities listed in Table 5-1.

Table 5-1 RAR Protocols

Feature	RFC 5578	Dynamic Link Exchange Protocol (DLEP)
Transport	Point-to-Point Protocol over Ethernet (PPPoE)	UDP
Packet Transport	Point-to-Point Point to Multipoint	Broadcast Multi-access
Flow Control	Credit or Rate-based	Rate-based
Convergence Events	Yes	Yes
Metrics	Defined in RFC 5578	Same metrics as RFC 5578
Modem Support	Split-stack PPPoE to router	UDP to router Transparent bridge on data path
RFC Status	Informational	Standards-track (submitted, not yet approved)
Supports Modem Multiple Hops from Router	No, PPPoE discovery is broadcast	Yes
Open Source	Available for client only	Available for both client and server
See Chapter	Chapter 8, "Configuring PPPoE"	Chapter 6, "Understanding and Configuring DLEP"

Table 5-2 lists the routing protocols that support RAR and MANET:

Table 5-2 Routing Protocols that Support RAR and MANET

Routing Protocol	See Chapter
Open Shortest Path First, Version 3 (OSPFv3)	Chapter 10, "Configuring OSPFv3 for a MANET"
Enhanced Interior Gateway Routing Protocol (EIGRP)	Chapter 11, "Configuring EIGRP in a MANET"

Understanding Virtual Templates

Each RAR protocol requires a virtual template. The virtual template is used to create Virtual-Access interfaces. All Virtual-Access interfaces inherit the attributes of the virtual template. When configuring each RAR protocol, you will assign a virtual-template number. To configure virtual templates for each RAR protocol, see the chapter in this manual on the specific protocol.

Configuring QoS

When using RAR, QoS is applied at the Virtual-Access interfaces. Defining and enforcing QoS profiles is configured on a next-hop basis. Traffic prioritization to one peer system should not impact traffic prioritization to other peers.

Configuring Quality of Service (QoS) varies per protocol:

- MQC—For RFC 5578, DLEP, and Modular QoS CLI (MQC) configurations are supported. Full MQC configurations include remarking, shaping, and policing.
- CDR-based QoS—For DLEP and QoS configuration is based entirely on Current Data Rate (CDR) shaping.

  For more information about CDR-based QoS configurations, see CDR-based QoS, page 5-3.

QoS Configuration Types

Configuring Quality of Service (QoS) can follow one of various approaches:

- CDR-based QoS, page 5-3
- Standard IOS QoS, page 5-3

CDR-based QoS

The only QoS configuration required for DLEP or R2CP is the shaping definition. When DLEP or R2CP detects a new neighbor, a set of metrics is exchanged from radio to router. These metrics include a Current Data Rate (CDR) value. When configuring rate-based shaping, the router shapes the traffic destined for each neighbor based on its CDR rate.

Reporting CDR Values

When using rate-based shaping, the parent policy includes a percent value for the shaping command. This allows the radio to report a different CDR value and the shaping to adapt to the new value on the router. While you can use a static bandwidth on the shaping command, it may not represent the link properly, resulting in traffic that can queue unpredictably.

Traffic Queues

Traffic queues are based on the child policy-map while the parent policy-map shapes the traffic. Most of the configuration is a normal hierarchical configuration.

For more information on normal hierarchical configuration, go to the following URL:
http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_mqc_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Standard IOS QoS

Standard QoS configuration requires the following:

1. Traffic Class Configuration, page 5-4
2. Policy Map Configuration, page 5-4

3. Policy Assignment, page 5-4

For general information on configuring QoS, go to the following URL:
http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_mqc.pdf

Traffic Class Configuration

You must configure traffic classes for QoS. Traffic classes contain a traffic class name, a match command, and instructions on how to evaluate match commands. Once configured, you can assign the QoS policy to the Virtual-Access interface.

For information on how to configure classes, refer to the following URL:
http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_mqc.ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1058823

Policy Map Configuration

You must configure policy maps for QoS. After configuring policies, you can attach the policies to a Virtual-Access interface.

For information on how to configure policies, refer to the following URL:
http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_mqc.ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1059601

Policy Assignment

After configuring traffic classes and policy maps, you can assign policies to the virtual interface. You assign policies to the Virtual-Access interface to apply QoS shaping to the previously created virtual template. Policies are applied to every peer that the RAR protocol creates.

For information on how to assign policies to the virtual template, refer to the following URL:
http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_mqc.ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp105970

CHAPTER 6

Understanding and Configuring DLEP

After configuring the interfaces and verifying connectivity as described in Chapter 3, “Configuring the Interfaces,” the next step is to configure the protocols for those interfaces. The Dynamic Link Exchange Protocol (DLEP) is a radio aware routing (RAR) protocol.

Prerequisite Reading

Read Chapter 5, “Introduction to Radio Aware Routing and MANET” before selecting the appropriate protocol per each interface configured in Chapter 3, “Configuring the Interfaces,”.

Note See Appendix A, “Command Reference” for detailed command reference.

Configuring DLEP

This chapter provides the following major sections for initiating, verifying, and managing all aspects of Dynamic Link Exchange Protocol (DLEP) on an interface:

- Configuring the Physical Interface, page 6-1
- Disabling Virtual Template Subinterfaces, page 6-3
- Creating the Virtual Template, page 6-3
- Configuring the VMI, page 6-4
- Verifying DLEP Configuration, page 6-6
- Technical Support for DLEP, page 6-7

Configuring the Physical Interface

In addition to configuring a description, IP address, and other interface characteristics, you must specify that the physical interface use a virtual template which is the source for all of the DLEP Virtual-Access interfaces.

To configure the virtual template for an interface, perform the following procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **intereface FastEthernet0/1**
4. **description** *description*
5. **ip address** *A.B.C.D a.b.c.d*
6. **no ip proxy-arp**
7. **ip dlep vtemplate** *number*
8. **duplex auto**
9. **speed auto**
10. **ipv6 enable**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
	`Enter configuration commands, one per line.`
	`End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	`interface fastethernet`*`number`*
	Example:
	`Router(config)# interface fastethernet0/1`
	`Router(config-if)#`
		Enters interface configuration mode.

Step 4	`description` *`description`*
	Example:
	`Router(config-if)#description DLEP RADIO CONNECTION`
		Specifies a description for the interface.
		In this example, the description is DLEP RADIO CONNECTION.

	Command or Action	Purpose

Step 5	`ip address` *`A.B.C.D a.b.c.d`*
	Example:
	`Router(config-if)#ip address 10.10.10.4 255.255.255.0`
		Specifies the IP address and subnet mask for the physical interface.
		In this example, the IP address is set to10.10.10.4 and the subnet mask is 255.255.255.0.

Step 6	`no ip proxy-arp`
	Example:
	`Router(config-if)#no ip proxy-arp`
		Prevents the interface from responding to ARP requests for other routers on the interface.
		This command is required for DLEP.

Step 7	`ip dlep vtemplate` *`number`* `port` *`number`*
	Example:
	`Router(config-if)#ip dlep vtemplate number 13`
		Initiates DLEP on the interface by setting the virtual-access template number and optional port number. The valid values for the templates range from 1 to 4096.
		The valid values for the port number range from 1 to 65534. If you do not specify a port number, Port number 55555 is used be default.

Step 8	`duplex auto`	Configures the interface to automatically set up duplexing.
Step 9	`speed auto`	Configures the interface to automatically negotiate with the corresponding interface and set the communication speed.
Step 10	`ipv6 enable`	Enables IPv6 on the interface.

Step 11	`exit`
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits the current mode.

Disabling Virtual Template Subinterfaces

By default, Cisco IOS configures virtual-access interfaces as subinterfaces. You must enter the **no virtual-template subinterface** command so that the virtual access interfaces are not configured as sub-interfaces.

Creating the Virtual Template

Perform this task to create the DLEP virtual template:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface Virtual-Template** *number*
4. **ip unnumbered FastEthernet0/1**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
	`Enter configuration commands, one per line.`
	`End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**`interface Virtual-Template`** *`number`*
	Example:
	`Router(config)# interface Virtual-Template 13`
	`Router(config-if)#`
		Creates a virtual template for DLEP.
		This example creates virtual template 13.

Step 4	**`ip unnumbered FastEthernet0/1`**
	Example:
	`Router(config-if)#ip unnumbered FastEthernet0/1`
		Specifies the physical interface where the VMI retrieves the IP address for the physical interface.

Step 5	**`exit`**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits the current mode.

Configuring the VMI

The VMI is the upper level in the RAR environment that communicates with the routing protocols. It is important to set the IP address to unnumbered and to the physical interface so that the VMI knows where to get the IP address for each virtual-access interface.

It is equally important to set the physical interface correctly, so that DLEP knows where to insert the packets for delivery.

To configure the VMI, perform the following procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **intereface vmi** *number*
4. **ip unnumbered FastEthernet0/1**
5. **physical-interface Fast-Ethernet0/1**

6. **ipv6 enable**
7. **ospfv3 1 network manet**
8. **ospfv3 1 area0**
9. **ospfv3 2 network manet**
10. **ospfv3 2 area 0 ipv4**
11. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router>` **`enable`**
	`Router#`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router#` **`configure terminal`**
	`Enter configuration commands, one per line.`
	`End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**`interface vmi`** *`number`*
	Example:
	`Router(config)#` **`interface vmi1`**
	`Router(config-if)#`
		Creates a VMI and enters interface configuration mode.
		This example creates VMI1.

Step 4	**`ip unnumbered FastEthernet0/1`**
	Example:
	`Router(config-if)#`**`ip unnumbered FastEthernet0/1`**
		Specifies the physical interface where the VMI retrieves the IP address for the physical interface.

Step 5	**`physical-interface FastEthernet0/1`**
	Example:
	`Router(config-if)#`**`physical-interface`**
	`FastEthernet0/1`
		Specifies where the Virtual-Access interface inserts packets for delivery.

Step 6	**`ipv6 enble`**	Enables IPv6 on the VMI.

	Command or Action	Purpose

Step 7	**Example:**
	`Router(config-if)#`**`ospfv3 1 network manet`**
	`Router(config-if)#`**`ospfv3 1 area 0`**
	`Router(config-if)#`**`ospfv3 2 network manet`**
	`Router(config-if)#`**`ospfv3 area 0 ipv4`**
		Configure the routing protocols for your network. These commands will vary depending on the routing protocol for the network.
		This example configures ospfv3 as the routing protocol using manet as the network type, and uses address families for IPv4 addressing.

Step 8	**`exit`**
	Example:
	`Router(config-if)#` **`exit`**
	`Router(config)#`
		Exits the current mode.

Configuring Optional Timers

DLEP has several optional timers that you can configure. Cisco recommends that you use the defaults settings for these timers. These commands are documented in the Appendix A, "Command Reference."

Verifying DLEP Configuration

The following examples show how to verify DLEP configuration on the router interface:

- Displaying Information for DLEP Clients, page 6-7
- Displaying DLEP Router Configuration, page 6-7
- Displaying Neighbors on a DLEP Interface, page 6-7

Note You can display general information as in the following examples:

- For DLEP clients:

```
Router> show dlep clients ?
FastEthernet  FastEthernet IEEE 802.3
  Vlan          Vlan IEEE 802.1q
  |             Output modifiers
  <cr>
```

- For the DLEP server configuration:

```
Router> show dlep config ?
FastEthernet  FastEthernet IEEE 802.3
  Vlan          Vlan IEEE 802.1q
  |             Output modifiers
  <cr>
```

- For DLEP neighbors:

```
Router> show dlep neighbors ?
FastEthernet  FastEthernet IEEE 802.3
  Vlan          Vlan IEEE 802.1q
  |             Output modifiers
  <cr>
```

Displaying Information for DLEP Clients

This example shows how to display router-to-radio peer associations on DLEP interfaces.

```
Router> show dlep clients

DLEP Clients for all interfaces:


DLEP Clients for Interface FastEthernet0/1
DLEP Server IP=12.12.12.101:55555 Sock=1


DLEP Client IP=12.12.12.7:38681
 Peer ID=1, Virtual template=13
 Description: DLEP_Radio_Sim_1
 Peer Timers (all values in seconds):
  Heartbeat=10, Dead Interval=40, Terminate ACK=10
 Neighbor Timers (all values in seconds):
  Activity timeout=0, Neighbor Down ACK=10
```

Displaying DLEP Router Configuration

This example shows how to display configuration details for the DLEP server configuration:

```
Router> show dlep config
DLEP Configuration for FastEthernet0/1.5

DLEP Server IP=10.10.5.4:55555
 Virtual template=13
 Missed heartbeat threshold=4, Peer Terminate ACK timeout=10
 Neighbor activity timeout=0, Neighbor Down ACK timeout=10
```

Displaying Neighbors on a DLEP Interface

This example shows how to display information about established neighbor sessions on DLEP interfaces.

```
Router> show dlep neighbors
DLEP Neighbors for Interface FastEthernet0/1
DLEP Server IP=12.12.12.101:55555 Sock=1


SID=2150  MAC_Address=1122.3344.5566
  Addresses:
  No Layer 3 addresses are specified.
  Metrics:  rlq=100  resources=100  latency=250 milliseconds
            cdr=100000000 bps  mdr=100000000 bps
```

Technical Support for DLEP

Contact your Cisco Support engineer for any troubleshooting support you may need. The following information is available for your reference:

- Debug Commands, page A-1
- Default Settings for DLEP, page C-1

Caution We do not recommend that you change the default DLEP configuration unless a Cisco Support engineer instructs you to do so.

CHAPTER 7

Configuring R2CP

After configuring the interfaces and verifying connectivity as described in Chapter 3, "Configuring the Interfaces," the next step is configuring the protocols for those interfaces.

Note R2CP is not available on the Cisco 5921 ESR.

Prerequisite Reading

Read the following chapters before selecting the appropriate protocol per interface:

- Chapter 5, "Introduction to Radio Aware Routing and MANET"

Note See Appendix A, "Command Reference" for detailed command reference.

R2CP Configuration

This chapter provides the following major sections for initiating, verifying, and managing all aspects of R2CP on an interface:

- Configuring R2CP on the Router, page 7-1
- Verifying R2CP Configuration, page 7-10

Configuring R2CP on the Router

When configuring R2CP on the router you must perform the following tasks:

- Configuring the Heartbeat Threshold, page 7-2
- Configuring the Node Terminate ACK Threshold, page 7-3
- Configuring the Node Terminate ACK Timeout, page 7-4
- Configuring the Port Number for the Server, page 7-5
- Configuring the Session Activity Timeout, page 7-6
- Configuring the Session Terminate ACK Threshold, page 7-7

- Configuring the Session Terminate ACK Timeout, page 7-8
- Configuring the Virtual Access Template Number, page 7-9

Note You must perform all tasks to properly configure R2CP on the router.

Configuring the Heartbeat Threshold

Perform this task to configure the heartbeat threshold on the router. The heartbeat threshold determines the number of heartbeats allowed by R2CP before declaring a failed association.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type slot/port*]
4. **ip r2cp heartbeat-threshold** *count*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router>` **`enable`**
	`Router#`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router#` **`configure terminal`**
	`Enter configuration commands, one per line.`
	`End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**`interface`** `[`*`type slot/port`*`]`
	Example:
	`Router(config)#` **`interface fastEthernet 0/1`**
	`Router(config-if)#`
		Enters interface configuration mode.

	Command or Action	Purpose

Step 4	`ip r2cp heartbeat-threshold` *count*
	Example:
	`Router(config-if)# ip r2cp heartbeat-threshold 3`
	`Router(config-if)#`
		Sets the heartbeat-threshold. The heartbeat-threshold ranges between 2 and 8.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits the current mode.

Configuring the Node Terminate ACK Threshold

Perform this task to configure the node terminate acknowledgement (ACK) threshold. You configure the node terminate acknowledgement threshold to set the number of missed and/or lost node acknowledgements performed before declaring the terminate effort complete.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type slot/port*]
4. **ip r2cp node-terminate-ack-threshold** *value*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 3	**interface** [*type slot/port*]
	
	Example:
	`Router(config)# interface fastEthernet 0/1`
	`Router(config-if)#`
		Enters interface configuration mode.

Step 4	**ip r2cp node-terminate-ack-threshold** *value*
	
	Example:
	`Router(config-if)# ip r2cp node-terminate-ack-threshold 2`
	`Router(config-if)#`
		Sets the node terminate acknowledgement (ACK) threshold. The node-terminate ACK threshold ranges between 1 and 5.

Step 5	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits the current mode.

Configuring the Node Terminate ACK Timeout

Perform this task to configure the node terminate acknowledgement timeout. You configure the node terminate acknowledgement timeout to set the duration allowed when waiting for the node terminate acknowledgement.

Note The duration of the node terminate acknowledgement timeout is set in milliseconds.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type slot/port*]
4. **ip r2cp node-terminate-ack-timeout** *milliseconds*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable** Router#	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enters global configuration mode.
Step 3	**interface** [*type slot/port*] **Example:** Router(config)# **interface fastEthernet 0/1** Router(config-if)#	Enters interface configuration mode.
Step 4	**ip r2cp node-terminate-ack-timeout** *milliseconds* **Example:** Router(config-if)# **ip r2cp** **node-terminate-ack-timeout 2200** Router(config-if)#	Sets the node terminate acknowledgement timeout. The node-terminate ACK timeout ranges between 100 and 5000 milliseconds.
Step 5	**exit** **Example:** Router(config-if)# **exit** Router(config)#	Exits the current mode.

Configuring the Port Number for the Server

Perform this task to configure the port number for the server. You configure the port number for the server to set the port number on which the server listens.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type slot/port*]
4. **ip r2cp port** *number*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable** Router#	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enters global configuration mode.
Step 3	**interface** [*type slot/port*] **Example:** Router(config)# **interface fastEthernet 0/1** Router(config-if)#	Enters interface configuration mode.
Step 4	**ip r2cp port** *number* **Example:** Router(config-if)# **ip r2cp port 5858** Router(config-if)#	Sets the port number on which the server listens. The port number ranges between 1 and 65534.
Step 5	**exit** **Example:** Router(config-if)# **exit** Router(config)#	Exits the current mode.

Configuring the Session Activity Timeout

Perform this task to configure the session activity timeout. You configure the session activity timeout to set a guard timer duration in order to catch stale sessions. The session activity timeout terminates when the timer expires.

Note The duration of the session activity timeout is set in seconds.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type slot/port*]
4. **ip r2cp session-activity-timeout** *seconds*

5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable** Router#	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enters global configuration mode.
Step 3	**interface** [*type slot/port*] **Example:** Router(config)# **interface fastEthernet 0/1** Router(config-if)#	Enters interface configuration mode.
Step 4	**ip r2cp session-activity-timeout** *seconds* **Example:** Router(config-if)# **ip r2cp** session-activity-timeout 2 Router(config-if)#	Sets the session activity timeout. The session activity guard timer ranges between 0 and 4 seconds.
Step 5	**exit** **Example:** Router(config-if)# **exit** Router(config)#	Exits the current mode.

Configuring the Session Terminate ACK Threshold

Perform this task to configure the session terminate acknowledgement threshold. You configure the session terminate acknowledgement threshold to set the number of missed and/or lost session acknowledgements allowed before declaring the terminate effort complete.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type slot/port*]
4. **ip r2cp session-terminate-ack-threshold** *value*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
	`Enter configuration commands, one per line.`
	`End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**`interface`** `[`*`type slot/port`*`]`
	Example:
	`Router(config)# interface fastEthernet 0/1`
	`Router(config-if)#`
		Enters interface configuration mode.

Step 4	**`ip r2cp session-terminate-ack-threshold`** *`value`*
	Example:
	`Router(config-if)# ip r2cp`
	`session-terminate-ack-threshold 4`
	`Router(config-if)#`
		Sets the threshold of missed session-terminate acknowledgements (ACKs). The session-terminate ACK threshold ranges between 1 and 5 sessions.

Step 5	**`exit`**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits the current mode.

Configuring the Session Terminate ACK Timeout

Perform this task to configure the session terminate acknowledgement timeout. You configure the session terminate acknowledgement timeout to set the time duration allowed when waiting for the session terminate acknowledgement.

Note The duration of the node terminate acknowledgement timeout is set in milliseconds.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type slot/port*]

4. **ip r2cp session-terminate-ack-timeout** *milliseconds*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
	`Enter configuration commands, one per line.`
	`End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	`interface [type slot/port]`
	Example:
	`Router(config)# interface fastEthernet 0/1`
	`Router(config-if)#`
		Enters interface configuration mode.

Step 4	`ip r2cp session-terminate-ack-timeout milliseconds`
	Example:
	`Router(config-if)# ip r2cp session-terminate-ack-timeout 2400`
	`Router(config-if)#`
		Sets the session-terminate ACK guard timer duration. The session-terminate ACK timeout ranges between 100 and 5000 milliseconds.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits the current mode.

Configuring the Virtual Access Template Number

Perform this task to configure the virtual access template number. You configure the virtual access template number to determine which virtual template to use when creating the virtual access interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type slot/port*]
4. **ip r2cp virtual-template** *number*

5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
	`Enter configuration commands, one per line.`
	`End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	`interface [type slot/port]`
	Example:
	`Router(config)# interface fastEthernet 0/1`
	`Router(config-if)#`
		Enters interface configuration mode.

Step 4	`ip r2cp virtual-template number`
	Example:
	`Router(config-if)# ip r2cp virtual-template 224`
	`Router(config-if)#`
		Sets the virtual access template number. The virtual access template number ranges between 0 and 21474883647.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits the current mode.

Verifying R2CP Configuration

The following procedures are available for verifying the R2CP configuration on the router:

- Displaying Radio Clients on an R2CP Interface, page 7-11
- Displaying R2CP Router Configuration, page 7-12
- Displaying Neighbors on an R2CP Interface, page 7-12

Note You can show general details related to Fast Ethernet, VLAN, and output modifiers for all R2CP clients.

Example

General R2CP Client Details

The following example shows how to display general radio client details:

```
Router> show r2cp clients ?
FastEthernet  FastEthernet IEEE 802.3
  Vlan          Vlan IEEE 802.1q
  |             Output modifiers
  <cr>
```

Displaying Radio Clients on an R2CP Interface

You show radio clients to exchange metric information with the radio for either all radio clients on all interfaces or for one radio client on a specific interface.

Examples

All Radio Clients on all Interfaces

The following example shows how to display all radio clients on all interfaces:

```
Router> show r2cp clients
R2CP Clients for all interfaces:

R2CP Clients for Interface FastEthernet0/1
R2CP Server IP=12.12.12.101:28672 Sock=1

R2CP Client ID=1 IP=12.12.12.7:5500
 node heartbeat missed count=0
 node heartbeat interval=5 seconds
 node heartbeat missed threshold=3
 node terminate ack missed count=0
 node terminate ack timeout=1000 milliseconds
 node terminate ack missed threshold=3
 session activity timeout=1 minutes
 session terminate ack timeout=1000 milliseconds
 session terminate ack missed threshold=3
No Virtual Template defined.
```

One Radio Client on a Specific Interface

The following example shows how to display one radio client on a specific interface:

```
Router> show r2cp fastEthernet 0/1
r2cp clients fastEthernet 0/1

R2CP Clients for Interface FastEthernet0/1
R2CP Server IP=12.12.12.101:28672 Sock=1

R2CP Client ID=1 IP=12.12.12.7:5500
 node heartbeat missed count=0
 node heartbeat interval=5 seconds
 node heartbeat missed threshold=3
 node terminate ack missed count=0
 node terminate ack timeout=1000 milliseconds
 node terminate ack missed threshold=3
 session activity timeout=1 minutes
 session terminate ack timeout=1000 milliseconds
 session terminate ack missed threshold=3
 No Virtual Template defined.
```

Displaying R2CP Router Configuration

You can display router configuration information details for the R2CP interface. These configuration details include the following components:

- Heartbeat threshold
- Node-terminate acknowledgement (ACK) threshold
- Node-terminate ACK timeout
- Port number
- Session-activity timeout
- Session-terminate ACK threshold
- Session-terminate ACK timeout
- Virtual-access template number

Example

Displaying R2CP Router Configuration

The following example shows how to display configuration details for the R2CP interface:

```
Router> show r2cp config
R2CP Configuration from FastEthernet0/1

R2CP Server IP=12.12.12.101:28672
 node heartbeat missed threshold=3
 node terminate ack timeout=2200 milliseconds
 node terminate ack missed threshold=2
 session activity timeout=3 minutes
 session terminate ack timeout=1000 milliseconds
 session terminate ack missed threshold=5
 virtual template=220
```

Displaying Neighbors on an R2CP Interface

You show neighbors on an R2CP interface to display information about the neighbors with which the radio can talk from a Layer 3, next-hop perspective. Show R2CP neighbors allows you to get metric data associated with a next-hop, so you can better understand the paths that the traffic is taking.

Example

Displaying Two Radio Neighbors/Sessions

This example shows how to display a configuration that includes two radio neighbors/sessions:

```
Router> show r2cp neighbors

R2CP Neighbors for all interfaces:

R2CP Neighbors for Interface FastEthernet0/1
R2CP Server IP=12.12.12.101:28672 Sock=1

  Global Session ID=101
 MAC Address: 1122.3344.5566
 Vlan ID: 0
```

```
Metrics:  rlq=100  resources=100  latency=10 milliseconds
          cdr=100000 Kbps  mdr=100000 Kbps
 Global Session ID=102
MAC Address: 2222.3344.5566
Vlan ID: 0
Metrics:  rlq=100  resources=100  latency=10 milliseconds
          cdr=100000 Kbps  mdr=100000 Kbps
```

CHAPTER 8

Configuring PPPoE

After configuring the interfaces and verifying connectivity as described in Chapter 3, "Configuring the Interfaces," the next step is configuring the protocols.

Prerequisite Reading

Read the following chapter before selecting a RAR protocol:

- Chapter 5, "Introduction to Radio Aware Routing and MANET"

Note You can use only one RAR protocol per interface.

This chapter contains the following sections:

- PPPoE in a MANET, page 8-1
- VMI in a MANET, page 8-2
- PPPoE and VMI, page 8-6
- Configuring PPPoE for use with VMI, page 8-7
- Showing VMI Neighbors, page 8-18

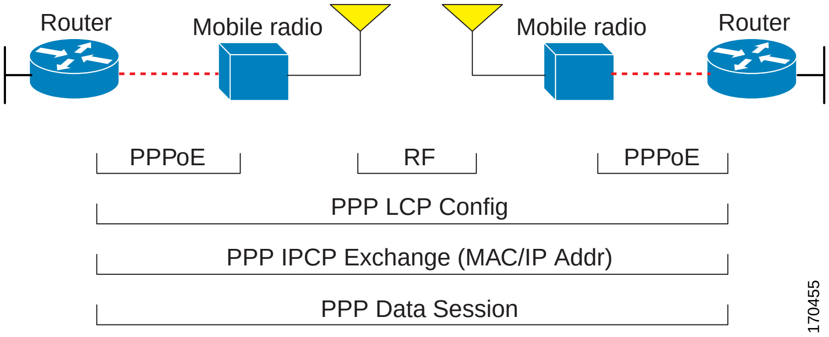
PPPoE in a MANET

The Cisco MANET solution employs PPPoE sessions to enable intra-nodal communications between a router and its partner radio. Each radio initiates the PPPoE session as soon as the radio establishes a radio link to another radio. After the PPPoE sessions are active, a PPP session is established end-to-end (router-to-router.) This is duplicated each time a radio establishes a new radio link. VMI on the router can aggregate multiple PPPoE sessions and multiplex them to look like a single interface to the routing processes. Underneath VMI are virtual access interfaces that are associated with each of the PPP/PPPoE connections.

If you are running multicast applications that require the virtual-access interfaces to be exposed to applications above L2 directly, you can configure VMI to operate in bypass mode. Most multicast applications require that the virtual-access interfaces be exposed directly to the routing protocols to ensure that multicast Reverse Path Forwarding (RPF) can operate as expected. When you use the bypass mode, you must define a VMI to handle presentation of cross-layer signals such as neighbor up, neighbor down, and metrics. Applications are aware of the actual underlying virtual-access interfaces and send packets to the underlying virtual-access interfaces directly. Additional information is required on the virtual template configuration. Operating VMI in bypass mode can cause databases in the applications to be larger than would normally be expected because knowledge of more interfaces is required for normal operation.

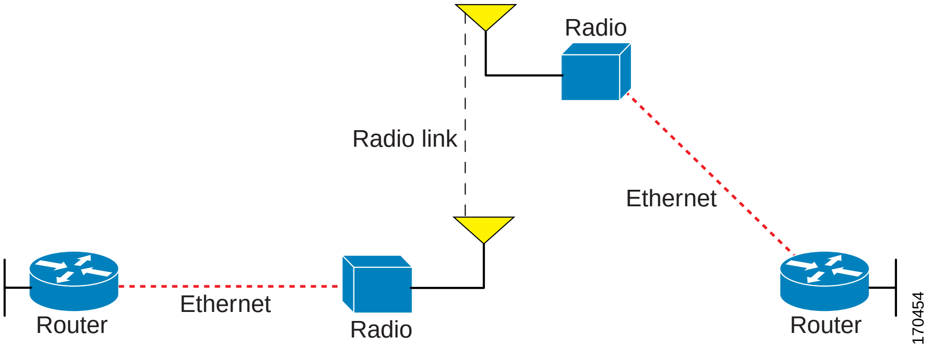
A PPPoE session is established between a router and a radio on behalf of every other router/radio neighbor located in the MANET. These L2 sessions are the means by which radio network status gets reported to the Layer 3 (L3) processes in the router. Figure 8-1 illustrates the PPPoE session exchange between mobile routers and directional radios in a MANET.

Figure 8-1 PPPoE Session Exchange Between Mobile Routers and Directional Radios



This capability requires that an RFC-5578 compliant radio be connected to a router using Ethernet. The router always considers the Ethernet link to be up. If the radio side of the link goes down, the router waits until a routing update time-out occurs to declare that the route is down and then updates the routing table. Figure 8-2 illustrates a simple router-to-radio link topology. The routing protocols optimized for VMI PPPoE are EIGRP (IPv4, IPv6) and OSPFv3 (IPv4, IPv6).

Figure 8-2 Router-to-Radio Link



VMI in a MANET

VMI provides services that map outgoing packets to the appropriate PPPoE sessions based on the next-hop forwarding address for that packet. VMI also provides a broadcast service that emulates a set of point-to-point connections as a point-to-multipoint interface with broadcast ability. When a packet with a multicast address is forwarded through VMI in aggregate mode, VMI replicates the packet and sends it using the virtual-access interface(s) to each of its neighbors.

Directional radios are frequently used in applications that require greater bandwidth, increased power-to-transmission range, or reduced probability of detection. These radios operate in a point-to-point mode, and generally have no broadcast capability. On the other hand, the routing processes in Cisco's MANET solution operate most efficiently when viewing the network link as point-to-multipoint, with broadcast capability. For the router, modeling the MANET as a collection of point-to-point nodes has a dramatic impact on the size of its internal database.

VMI within the router can aggregate all of the per-neighbor PPPoE sessions from the Radio Ethernet connection. VMI maps the sessions to appear to L3 routing protocols and applications as a single point-to-multipoint, multi-access, broadcast-capable network. However, VMI preserves the integrity of the PPPoE sessions on the radio side, so that each point-to-point connection can have its own Quality of Service (QoS) queue.

VMI also relays the link quality metric and neighbor up/down signaling from the radio to the routing protocols. Currently, VMI signals are used by Enhanced Interior Gateway Routing Protocol (EIGRP) (for IPv4 and IPv6 neighbors) and OSPFv3 (for IPv6 neighbors).

Link-Quality Metrics

The quality of a radio link has a direct impact on the throughput. The PPPoE protocol has been extended to provide a process by which a router can request report link quality metric information. Cisco's OSFPv3 and EIGRP implementations are enhanced so that the route cost to a neighbor is dynamically updated based on metrics reported by the radio, thus allowing the best route to be chosen within a given set of radio links.

The routing protocols receive raw radio link data, and compute a composite quality metric for each link. In computing these metrics, the router may consider the following factors:

- Maximum Data Rate—the theoretical maximum data rate of the radio link, in scaled bits per second
- Current Data Rate—the current data rate achieved on the link, in scaled bits per second
- Latency—the transmission delay packets encounter, in milliseconds
- Resources—a percentage (0-100) that can represent the remaining amount of a resource (such as battery power)
- Relative Link Quality—a numeric value (0-100) representing relative quality, with 100 being the highest quality

On the router, metrics can be weighted during the configuration process to emphasize or de-emphasize particular characteristics. For example, if throughput is a particular concern, you can weight the *throughput* metric so that it is factored more heavily into the composite route cost. Similarly, a metric of no concern can be omitted from the composite calculation.

Link metrics can change rapidly, often by very small degrees, which could result in a flood of meaningless routing updates. In a worst case scenario, the network churns almost continuously as it struggles to react to minor variations in link quality. To alleviate this concern, Cisco provides a tunable dampening mechanism that allows the user to configure threshold values. Any metric change that falls below the threshold is ignored.The quality of a connection to a neighbor varies, based on various characteristics of the interface when OSPFv3 or EIGRP is used as the routing protocol. The routing protocol receives dynamic raw radio link characteristics and computes a composite metric that is used to reduce the effect of frequent routing changes.

A tunable hysteresis mechanism allows you to adjust the threshold to the routing changes that occur when the router receives a signal that a new peer has been discovered, or that an existing peer is unreachable. The tunable metric is weighted and adjusted dynamically to account for the following characteristics:

- Current and Maximum Bandwidth
- Latency
- Resources
- Relative Link Quality (RLQ)

Individual weights can be deconfigured and all weights can be cleared so that the cost returns to the default value for the interface type. Based on the routing changes that occur, cost can be determined by the application of these metrics.

Neighbor Signaling

MANETs are highly dynamic environments. Nodes may move into, or out of, radio range at a fast pace. Each time a node joins or leaves the network, topology must be logically reconstructed by the routers. Routing protocols normally use timer-driven “hello” messages or neighbor time-outs to track topology changes, but MANETs reliance on these mechanisms can result in unacceptably slow convergence.

Neighbor up/down signaling capability provides faster network convergence by using link-status signals generated by the radio. The radio notifies the router each time a link to another neighbor is established or terminated by the creation and termination of PPPoE sessions. In the router, the routing protocols (OSPFv3 or EIGRP) respond immediately to these signals by expediting the formation of a new adjacency (for a new neighbor) or tearing down an existing adjacency (if a neighbor is lost). For example, if a vehicle drives behind a building and loses its connection, the router immediately senses the loss and establishes a new route to the vehicle through neighbors that are not blocked. This high speed network convergence is essential for minimizing dropped voice calls and disruptions to video sessions.

When VMI with PPPoE is used and a partner node has left or a new one has joined, the radio informs the router immediately of the topology change. Upon receiving the signal, the router immediately declares the change and updates the routing tables.

The signaling capability provides the following benefits:

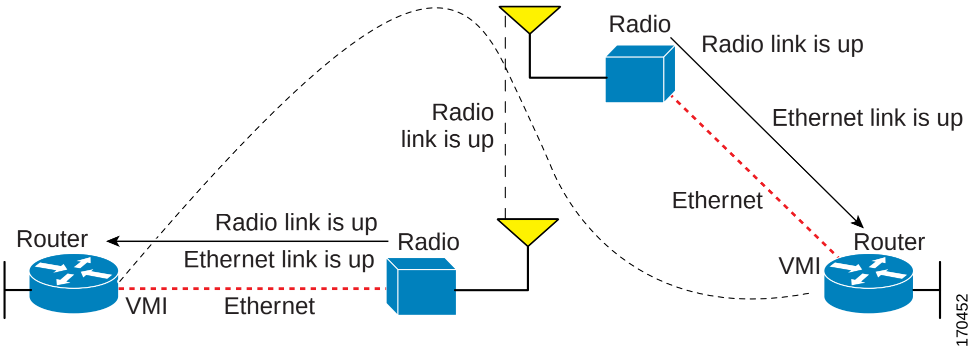
- Reduces routing delays and prevents applications from timing out
- Enables network-based applications and information to be delivered reliably and quickly over directional radio links
- Provides faster convergence and optimal route selection so that delay-sensitive traffic such as voice and video are not disrupted
- Reduces impact on radio equipment by minimizing the need for internal queuing/buffering
- Provides consistent Quality of Service (QoS) for networks with multiple radios

The messaging allows for flexible rerouting when necessary because of the following conditions:

- Noise on the Radio links
- Fading of the Radio links
- Congestion of the Radio links
- Radio link power fade
- Utilization of the Radio

Figure 8-3 illustrates the signaling sequence that occurs when radio links go up and down.

Figure 8-3 Up and Down Signaling Sequence



PPPoE Credit-based Flow Control

Each radio initiates a PPPoE session with its local router as soon as the radio establishes a link to another radio. Once the PPPoE sessions are active for each node, a PPP session is then established end-to-end (router-to-router). This process is duplicated each time a radio establishes a new link.

The carrying capacity of each radio link may vary due to location changes or environmental conditions, and many radio transmission systems have limited buffering capabilities. To minimize the need for packet queuing in the radio, Cisco has implemented extensions to the PPPoE protocol that enable the router to control traffic buffering in congestion situations. Implementing flow-control on these router-to-radio sessions also allows the use of fair queuing.

The flow control solution utilizes a credit-granting mechanism documented in RFC 5578. When the PPPoE session is established, the radio can request a flow-controlled session. If the router acknowledges the request, all subsequent traffic must be flow-controlled. If a flow control session has been requested and cannot be supported by the router, the session is terminated. Typically, both the radio and the router initially grant credits during session discovery. Once a device exhausts its credits, it must stop sending until additional credits have been granted. Credits can be added incrementally over the course of a session.

High performance radios that require high-speed links use metrics scaling. The radio can express the maximum and current data rates with different scaler values. Credit scaling allows a radio to change the default credit grant (or scaling factor) of 64 bytes to its default value. You can view the maximum and current data rates and the scalar value set by the radio from the output of the **show vmi neighbor detail** command.

Point-to-Point Protocol over Ethernet

Cross-layer feedback for router-radio integration radio aware routing takes advantage of the functions defined in RFC 5578. RFC 5578 is an Internet Engineering Task Force (IETF) standard that defines Point-to-Point Protocol over Ethernet (PPPoE) extensions for Ethernet-based communications between a router and a device such as a mobile radio that operates in a variable-bandwidth environment and has limited buffering capabilities. These extensions provide a PPPoE session based mechanism for sharing radio network status such as link-quality metrics and establishing flow control between a router and an RFC 5578-capable radio.

An RFC 5578 radio initiates an L2 PPPoE session with its adjacent router on behalf of every router and radio neighbor discovered in the network. These L2 sessions are the means by which radio network status for each neighbor link is reported to the router. The radio establishes correspondence between each PPPoE session and each link to a neighbor.

PPPoE and VMI

To use the PPPoE and Virtual Multipoint Interface (VMI) features described in this document, a radio device that implements the PPPoE functionality described in the RFC 2516 and RFC 5578 is required. OSPF enhancements are not tied to the PPPoE/VMI implementations, and as such do not require such radio devices.

VMI provides services that map outgoing packets to the appropriate PPPoE sessions based on the next-hop forwarding address for that packet. VMI also provides a broadcast service that emulates a set of point-to-point connections as a point-to-multipoint interface with broadcast ability. When a packet with a multicast address is forwarded through VMI in aggregate mode, VMI replicates the packet and sends it using the virtual-access interface(s) to each of its neighbors.

Note VMI operates in aggregate mode by default. This release supports VMI in aggregate mode and also in bypass mode.

Directional radios are frequently used in applications that require greater bandwidth, increased power-to-transmission range, or reduced probability of detection. These radios operate in a point-to-point mode, and generally have no broadcast capability.

Conversely, the routing processes in the Cisco MANET solution operate most efficiently when viewing the network link as point-to-multipoint with broadcast capability. For the router, modeling the MANET as a collection of point-to-point nodes has a dramatic impact on the size of its internal database.

VMI within the router can aggregate all of the per-neighbor PPPoE sessions from the radio Ethernet connection. VMI maps the sessions to appear to L3 routing protocols and applications as a single point-to-multipoint, multi-access, broadcast-capable network. However, VMI preserves the integrity of the PPPoE sessions on the radio side, so that each point-to-point connection can have its own Quality of Service (QoS) queue.

VMI also relays the link-quality metric and neighbor up/down signaling from the radio to the routing protocols. Currently, VMI signals are used by Enhanced Interior Gateway Routing Protocol (EIGRP) (for IPv4 and IPv6 neighbors) and OSPFv3 (for IPv6 neighbors).

Continuing with PPPoE Configuration

This chapter provides the following major sections to describe how to configure Point-to-Point Protocol over Ethernet (PPPoE) on a specific interface.

- Configuring PPPoE for use with VMI, page 8-7
- Showing VMI Neighbors, page 8-18

Note See Appendix A, “Command Reference” for detailed command reference.

Configuring PPPoE for use with VMI

This section provides the tasks required to configure PPPoE for use with Virtual Multipoint Interface (VMI):

- Creating a Subscriber Profile, page 8-7
- Configuring PPPoE Service Selection, page 8-8
- Configuring PPPoE on an Ethernet Interface, page 8-9
- Configuring a Virtual Template Interface, page 8-10
- Mapping Outgoing Packets, page 8-12
- Configuring Multicast Support, page 8-14

Creating a Subscriber Profile

Perform this task to configure a subscriber profile for PPPoE service selection.

Note Configuring a subscriber profile for PPPoE service selection is required for VMI to function properly.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **exit**
4. **subscriber authorization enable**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose

Step 3	`exit`
	Example:
	`Router(config-sss-profile)# exit`
		Returns to global configuration mode.

Step 4	`subscriber authorization enable`
	Example:
	`Router# subscriber authorization enable`
		Enable Subscriber Service Switch type authorization. This command is required when VPDN is not used.

Configuring PPPoE Service Selection

Perform this task to associate the subscriber profile with a PPPoE profile. In this configuration, the Broadband Access (BBA) group name must match the subscriber profile name defined in the subscriber profile.

Note In this example, *manet_radio* serves as the subscriber profile name.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **service profile** *subscriber-profile-name* [**refresh** *minutes*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`bba-group pppoe {group-name | global}`
	Example:
	`Router(config)# bba-group pppoe pppoe_group_1`
		Defines a PPPoE profile and enters BBA group configuration mode.

	Command or Action	Purpose
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies the virtual template required for cloning virtual-access interfaces. All PPPoE ports using this PPPoE profile will use this virtual template.
Step 5	**service profile** *subscriber-profile-name* [**refresh** *minutes*] **Example:** `Router(config-bba-group)# service profile subscriber_1`	Assigns a subscriber profile to a PPPoE profile. • The PPPoE server will advertise the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile.

Step 6	**end**
	Example:
	`Router(config-bba-group)# end`
		(Optional) Returns to privileged EXEC mode.

Configuring PPPoE on an Ethernet Interface

Perform this task to assign a PPPoE profile to an Ethernet interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type slot*/*port*]
4. **pppoe enable** [**group** *group-name*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**`interface`** [*`type slot/port`*] **Example:** `Router(config)# interface fastethernet 1/0`	Specifies an interface type and enters interface configuration mode. Valid interfaces include the following interface types: • Fast Ethernet interface • Ethernet • Fast Ethernet • Gigabit Ethernet • VLAN or VLAN subinterface
Step 4	**`pppoe enable`** [**`group`** *`group-name`*] **Example:** `Router(config-if)# pppoe enable group pppoe_group_1`	Enables PPPoE sessions on the interface or subinterface.

Step 5	**`end`**
	Example:
	`Router(config-if)# end`
		(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Configuring a Virtual Template Interface

Perform this task to configure a virtual-template interface. The virtual-template interface is required to clone configurations. For each VMI neighbor, a new virtual-access interface will be created dynamically.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no virtual-template subinterface**
4. **policy-map** *policy-map-name*
5. **class class-default**
6. **fair-queue**
7. **exit**
8. **interface virtual-template 1**
9. **ip unnumbered vmi1**
10. **service-policy output FQ**
11. **keepalive 60 20**
12. **end**

Detailed Steps

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`no virtual template subinterface`**
	Example:
	`Router# no virtual template subinterface`
		Disables the virtual template on the subinterface.

Step 4	**`policy-map`** *`policy-map-name`*
	Example:
	`Router(config-pmap)# policy-map FQ`
		Enters policy map configuration mode and creates, or modifies, a policy map that can be attached to one or more interfaces to specify a service policy.

Step 5	**`class class-default`**
	Example:
	`Router(config-pmap)# class class-default`
		Specifies one of the following:
		- Class Name for the policy you are about to create or change
		- Default Class (also known as a *Class-default Class*) for general policy configuration

Step 6	**`fair-queue`**
	Example:
	`Router(config-pmap)# fair-queue`
		Enables Weighted Fair Queueing (WFQ) in the policy-map.

Step 7	**`exit`**
	Example:
	`Router(config-pmap)# exit`
	`Router(config)#`
		Exits the current mode and returns to configuration mode.

Step 8	**`interface virtual-template`** *`number`*
	Example:
	`Router(config)# interface virtual-template 1`
		Creates a virtual-template interface for configuration and dynamic application to virtual-access interfaces.

Step 9	**`ip unnumbered`** *`interface-type interface-number`*
	Example:
	`Router(config-if)# ip unnumbered vmi1`
		Enables IP processing of IPv4 on the interface without assigning an explicit IP address.

Step 10	**`service-policy output`** `policy-map-name`
	Example:
	`Router(config-if)# service-policy output FQ`
		Attaches a policy map to an input interface, Virtual Circuit (VC), or output interface. This policy map will serve as the service policy for that interface or VC.

	Command or Action	Purpose
Step 11	**keepalive** [[keepalive-period] [keepalive-retries]] **Example:** `Router(config-if)# keepalive 60 20`	Enables a keepalive period of 60 seconds with 20 retries.

Step 12	**end**
	Example:
	`Router(config-if)# end`
		(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Example Configuration

```
no virtual-template subinterface
!
policy-map FQ
  class class-default
    fair-queue
!
interface Virtual-Template1
  ip unnumbered vmi1
  keepalive 60 20
  service-policy output FQ
!end
```

Mapping Outgoing Packets

Perform this task so that VMI can map outgoing packets to the appropriate PPPoE sessions. VMI will use the next-hop forwarding address from each outgoing packet perform this mapping.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vmi** *interface-number*
4. **ip address** *ip_addr subnet_mask*
5. **physical-interface** *interface-type/slot*
6. **end**

Detailed Steps

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface vmi** *number* **Example:** `Router(config)# interface vmi1`	Creates a VMI interface.
Step 4	**ip address** *ip_addr isubnet_mask* **Example:** `Router(config-if)# ip address 10.2.2.1 255.255.255.0`	Specifies the IP address and subnet mask for the VMI interface.
Step 5	**physical-interface** *interface-type/slot* **Example:** `Router(config-if)# physical-interface fa0/0`	Creates the physical subinterface to be associated with VMI on the router.

Step 6	**end**
	Example:
	`Router(config-if)# end`
		(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Examples

The following examples show the IP address coordination needed between virtual-template configuration and VMI configuration.

VMI in Aggregate Mode for IPv6

The following example shows the configuration of VMI in aggregate mode for IPv6.

```
interface Virtual-Template1
 ipv6 enable
 service-policy output FQ
!
interface vmi1
 ipv6 enable
 physical-interface FastEthernet0/0
!
```

VMI in Aggregate Mode for IPv4

The following example shows the configuration of VMI in aggregate mode for IPv4.

```
interface Virtual-Template1
 ip unnumbered vmi1
 service-policy output FQ
!
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 physical-interface FastEthernet0/0
!
```

VMI in Aggregate Mode for IPv4 and IPv6

The following example shows the configuration of VMI in aggregate mode for IPv4 and IPv6.

```
interface Virtual-Template1
 ip unnumbered vmi1
 ipv6 enable
 service-policy output FQ
!
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 ipv6 enable
 physical-interface FastEthernet0/0
!
```

Configuring Multicast Support

This section identifies the recommended modes and tasks for working with multicast:

- Using Aggregate Mode, page 8-14
- Using Bypass Mode, page 8-16
- Enabling Multicast Support on a VMI, page 8-16

Using Aggregate Mode

VMI operates in aggregate mode by default. All of the virtual-access interfaces created by PPPoE sessions are aggregated logically under the configured VMI. Applications above Layer 2 (L2), such as Enhanced Interior Gateway Routing Protocol (EIGRP) and OSPFv3, should be defined only on VMI. Packets sent to VMI are forwarded to the correct virtual-access interface(s). Aggregate mode VMIs operate in Non-Broadcast Multiple Access (NBMA) mode. Multicast traffic is forwarded only to the NBMA neighbors where a listener for that group is present. This is the preferred mode when operating in PIM sparse mode.

Note NBMA multicasting only supports IPv4 and sparse mode.

Perform this task to configure interface vmi1 to operate in NBMA mode and PIM sparse mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vmi** *interface-number*

4. **ip address** *ip_addr subnet_mask*
5. **ip pim nbma-mode**
6. **ip pim sparse-mode**
7. **load-interval** *number*
8. **physical-interface** `interface-type/slot`
9. **end**

Detailed Steps

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router>` **`enable`**
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router#` **`configure terminal`**
		Enters global configuration mode.

Step 3	**`interface vmi`** *`number`*
	Example:
	`Router(config)#` **`interface vmi1`**
		Creates a VMI interface.

Step 4	**`ip address`** *`ip_addr isubnet_mask`*
	Example:
	`Router(config-if)#` **`ip address 10.2.2.2 255.255.255.0`**
		Specifies the IP address and subnet mask for the VMI interface.
		This example sets the IP address to 10.2.2.2 and the subnet mask to 255.255.255.0

Step 5	**`ip pim nbma-mode`**	Enables NBMA mode.
Step 6	**`ip pim sparse-mod`**`e`	Enables sparse mode. **Note** You must set this to sparse mode.

Step 7	**`load interval`** *`seconds`*
	Example:
	`Router(config-if)#load-interval 30`
		Specifies the load interval in seconds.
		This example sets the load interval to 30 seconds.

Step 8	**`physical-interface`** *`interface-type/slot`*
	Example:
	`Router(config-if)#` **`physical-interface fa0/0`**
		Creates the physical subinterface to be associated with VMI on the router.

Step 9	**`end`**
	Example:
	`Router(config-if)#` **`end`**
		(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Using Bypass Mode

Using bypass mode is recommended for multicast applications.

In bypass mode, the virtual-access interfaces are directly exposed to applications running above L2. In bypass mode, you must still define a VMI because VMI continues to manage presentation of cross-layer signals, such as, neighbor up, neighbor down, and metrics. However, applications will still be aware of the actual underlying virtual-access interfaces and send packets to them directly.

Using bypass mode can cause databases in the applications to be larger because knowledge of more interfaces are required for normal operation.

If you are running multicast applications that require virtual-access interfaces to be exposed to applications above L2 directly, you can configure VMI to operate in bypass mode. Most multicast applications require that the virtual-access interfaces be exposed directly to routing protocols in order for the multicast Reverse Path Forwarding (RPF) to operate as expected. When you use the bypass mode, you must define a VMI to handle cross-layer signals such as neighbor up, neighbor down, and metrics. Applications will be aware of the actual underlying virtual-access interfaces, and will send packets to them directly. Operating VMI in bypass mode can cause databases in the applications to be larger than normally expected because knowledge of more interfaces is required for normal operation.

Enabling Multicast Support on a VMI

Perform this task to enable bypass mode on a VMI and override the default aggregation that occurs on VMI. This configuration assumes that you have already configured a virtual template and appropriate PPPoE sessions for VMI.

After you enter the enable bypass mode, Cisco recommends that you copy the running configuration to Non-Volatile Random Access Memory (NVRAM) because the default mode of operation for VMI is to logically aggregate the virtual-access interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *vmi number*
4. **mode bypass**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *vmi number* **Example:** Router(config-if)# **interface vmi1**	Enters interface configuration mode and relates a VMI interface.
Step 4	**mode bypass** **Example:** Router(config-if)# **mode bypass**	Overrides the default aggregation on the VMI interface and sets the mode to bypass to support multicast traffic on the interface.
Step 5	**exit** **Example:** Router(config-if)# **exit** Router(config)#	Exits the current mode.

Examples

Note VMI is required to have IP addresses assigned for VMI to work even though it will be shown as down/down while in bypass mode.

VMI in Bypass Mode for IPv6

The following example shows the configuration of VMI in bypass mode for IPv6.

```
interface Virtual-Template1
 ipv6 enable
 service-policy output FQ
!
interface vmi1
 ipv6 enable
 mode bypass
 physical-interface FastEthernet0/0
!
```

VMI in Bypass Mode for IPv4

The following example shows the configuration of VMI in bypass mode for IPv4.

Note The IPv4 address configured on VMI will not be advertised or used. Instead, the IPv4 address on the virtual-template will be used.

```
interface Virtual-Template1
 ip address 10.1.1.1 255.255.255.0
 service-policy output FQ
!
interface vmi1
 ip address 2.2.2.1 255.255.255.0
 mode bypass
 physical-interface FastEthernet0/0
!
```

VMI in Bypass Mode for IPv4 and IPv6

The following example shows the configuration of VMI in bypass mode for IPV4 and IPv6.

```
interface Virtual-Template1
 ip address 10.1.1.1 255.255.255.0
 ipv6 enable
 service-policy output FQ
!
interface vmi1
 ip address 2.2.2.1 255.255.255.0
 ipv6 enable
 mode bypass
 physical-interface FastEthernet0/0
!
```

Showing VMI Neighbors

To display information about neighbor connections to VMI, use the **show vmi neighbors** command in User EXEC mode.

The following example shows how to display neighbors created dynamically on a VMI:

```
Router# show vmi neighbors vmi1

1 vmi1 Neighbors

           IPV6       IPV4                    Transmit    Receive
Interface  Address    Address       Uptime      Packets     Packets
vmi1       ::         10.3.3.2      00:02:11    0000000008  0000000073
Router#
```

Example

The following example shows the details about known VMI neighbors.

```
Router# show vmi neighbors detail

            1 vmi1 Neighbors


vmi1   IPV6 Address=FE80::A8BB:CCFF:FE00:C00
       IPV4 Address=12.12.12.2, Uptime=00:12:19
       Output pkts=0, Input pkts=0
       METRIC DATA: Total rcvd=3, Avg arrival rate (ms)=234952
          CURRENT: MDR=2048000, CDR=1024000, Lat=70, Res=100, RLQ=95, load=1
          MDR      Max=10240000, Min=2048000, Avg=4795050
          CDR      Max=10240000, Min=1024000, Avg=4104192
          Latency  Max=1000, Min=70, Avg=380
          Resource Max=100, Min=100, Avg=100
          RLQ      Max=100, Min=95, Avg=96
          Load     Max=1, Min=1, Avg=1
       Transport PPPoE, Session ID=1
       INTERFACE STATS:
          VMI Interface=vmi1,
            Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2,
            Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=Ethernet0/0,
            Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
```

```
 Local Credits: 65296   Peer Credits: 65196
 Credit Grant Threshold: 28000    Max Credits per grant: 65534
 PADG Seq Num: 696     PADG Timer index: 0
 PADG last rcvd Seq Num: 697
 PADG last nonzero Seq Num: 0
 PADG last nonzero rcvd amount: 0
 PADG Timers:    [0]-1000    [1]-2000    [2]-3000    [3]-4000
 PADG xmit: 698  rcvd: 698
 PADC xmit: 698  rcvd: 698
 PADQ xmit: 0  rcvd: 2
Router#
```

CHAPTER 9

OSPFv3 Address Families

This chapter describes how to use OSPFv3 address families to route IPv6 packets over OSPFv3—using IPv4 or IPv6 addresses. This chapter also describes how to configure and use OSPFv3 address families in conjunction with Mobile Ad-hoc Network (MANETs) and Radio Aware Routing (RAR).

This chapter includes the following major sections:

- Configuring OSPFv3 Address Families, page 9-1
- Working with Multiple Address Families, page 9-10
- Redistributing IPv4 Routes, page 9-12
- Verifying OSPFv3 Address Families Configuration and Operation, page 9-13

OSPFv3 is defined to support IPv6 unicast prefixes. The Internet draft, *Support of Address Families in OSPFv3* (*IETF RFC 5838)*, extends OSPFv3 to support multiple address families. Cisco IOS implemented this extension, which allows IPv4 unicast addresses to be supported.

Configuring OSPFv3 Address Families

This section describes how to configure OSPFv3 Address Families for IPv6 and IPv4.

The Cisco OSPFv3 Address Families feature implements RFC 5838 and enables the ability to concurrently route IPv4 and IPv6 prefixes. The Cisco OSPFv3 Address Families feature is turned on in conjunction with the OSPFv3 MANET feature, which supports routing of IPv4 and IPv6 addresses and prefixes in mobile environments.

Configuring OSPFv3 Address Families is similar to configuring traditional IPv6 OSPFv3—the main difference being parameter usage in the CLI configuration commands. When configuring OSPFv3 Address Families, the new parameter `ospfv3` replaces the deprecated `ipv6 ospf` parameter.

Note See Appendix A, "Command Reference" for complete command reference information.

Working with IPv6 and OSPFv3 involves the following tasks:

1. Enabling IPv6, page 9-2
2. Enabling IPv6 on the Interface, page 9-3
3. Configuring OSPFv3 for a Unicast Address Family, page 9-3

Enabling IPv6

This task explains how to enable IPv6 routing, which is disabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`ipv6 unicast-routing`
	Example:
	`Router(config)# ipv6 unicast-routing`
		Enables the forwarding of IPv6 unicast datagrams.

Step 4	`exit`
	Example:
	`Router(config)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Enabling IPv6 on the Interface

This task explains how to enable IPv6 on an interface. This is a prerequisite to configuring OSPFv3 on the interface. IPv6 is disabled on the interface by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ipv6 enable**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface [type number]`
	Example:
	`Router(config)# interface ethernet 0/0`
		Specifies an interface type and number and places the router in interface-configuration mode.

Step 4	`ipv6 enable`
	Example:
	`Router(config-if)# ipv6 enable`
		Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Configuring OSPFv3 for a Unicast Address Family

Perform one of the following tasks:

- Configuring OSPFv3 for an IPv6 Unicast Address Family, page 9-4
- Configuring OSPFv3 for an IPv4 Unicast Address Family, page 9-6

Configuring OSPFv3 for an IPv6 Unicast Address Family

Configuring OSPFv3 for an IPv6 unicast address family involves the following tasks:

- Configuring the OSPFv3 IPv6 Address Family Instance on the Interface, page 9-4
- Configuring the OSPFv3 IPv6 Address Family Process, page 9-5

Configuring the OSPFv3 IPv6 Address Family Instance on the Interface

This task explains how to enable IPv6 packet forwarding and IPv6 routing. By default, both are disabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ospfv3** [*process-id*] **area** [*area-id*] **ipv6** [**instance** *instance-id*]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface [type number]`
	Example:
	`Router(config)# interface Ethernet 0/0`
		Configures an interface type.

Step 4	`ospfv3 [process-id] area [area-id] ipv6 [instance instance-id]`
	Example:
	`Router(config-if)# ospfv3 6 area 0 ipv6`
		Attaches the OSPFv3 process to an interface.
		Process ID: Valid range is 1 to 65535.
		Instance ID: 0 (Default value)
		The valid range is 0 to 31.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Example

The following is a configuration example:

```
version 15.1
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
ipv6 unicast-routing
!
interface Ethernet0/0
 ipv6 enable
 ospfv3 6 area 0 ipv6
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
!
router ospfv3 6
 router-id 6.6.6.6
 log-adjacency-changes
 address-family ipv6 unicast
 exit-address-family
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Configuring the OSPFv3 IPv6 Address Family Process

This task explains how to enable an OSPFv3 routing process and configure the address family.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **router-id** [*OSPFv3 router-id in IP address format*]
5. **address-family ipv6 unicast**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`router ospfv3 [process-id]`
	Example:
	`Router (config)# router ospfv3 6`
		Enables an OSPFv3 routing process to route IPv6 address-family traffic in IPv6 networks and enters router configuration mode.

Step 4	`router-id [OSPFV3 router-id in IP address format]`
	Example:
	`Router (config-rtr)# Router-id 10.1.1.1`
		Identifies a specific router rather than allowing the dynamic assignment of the router ID to occur.

Step 5	`address-family ipv6 unicast`
	Example:
	`Router(config-rtr)# address-family ipv6 unicast`
		Places the router in address family configuration mode for IPv6 address family.

Step 6	`exit`
	Example:
	`Router (config-router-af)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Configuring OSPFv3 for an IPv4 Unicast Address Family

Configuring an IPv4 unicast address family involves the following tasks:

1. Configuring the OSPFv3 IPv4 Address Family Instance on the Interface, page 9-7
2. Configuring an IPv4 Address on the Interface, page 9-8
3. Configuring the OSPFv3 IPv4 Address Family Process, page 9-9

Configuring the OSPFv3 IPv4 Address Family Instance on the Interface

This task explains how to enable IPv4 packet forwarding and IPv4 routing. By default, both are disabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ospfv3** [*process-id*] **area** [*area-id*] **ipv4** [**instance** *instance-id*]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface [type number]`
	Example:
	`Router(config)# interface Ethernet 0/0`
		Specifies the interface type and number and places the router in interface-configuration mode.

Step 4	`ospfv3 [process-id] area [area-id] ipv4 [instance instance-id]`
	Example:
	`Router(config-if)# ospfv3 4 area 0 ipv4`
		Configures the OSPFv3 process ID. The valid range is 1 to 65535.
		Optional—Instance ID: 64 (Default value)
		The valid range is 64 to 95.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Example

The following is a configuration example:

```
version 15.1
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
ipv6 unicast-routing
!
interface Ethernet0/0
 ip address 64.1.1.1 255.255.255.0
 ipv6 enable
 ospfv3 4 area 0 ipv4
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
!
router ospfv3 4
 router-id 4.4.4.4
 log-adjacency-changes
 address-family ipv4 unicast
 exit-address-family
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Configuring an IPv4 Address on the Interface

This task configures an IPv4 address on the interface. You can assign a primary IP address for a network interface.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface** [*type number*]
4. **ip address** [*ip address*] [*net mask*]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`router# configure terminal`
		Enters global configuration mode.

Step 3	`interface [type number]`
	Example:
	`Router(config)# interface ethernet 0/0`
		Specifies an interface type and number and places the router in interface configuration mode.

Step 4	`ip address [ip address] [net mask]`
	Example:
	`Router(config-if)# ip address 64.1.1.1 255.255.255.0`
		Assigns an IPv4 address to the interface.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Configuring the OSPFv3 IPv4 Address Family Process

This task explains how to enable an OSPFv3 routing process and configure the address family.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **router-id** [*OSPFv3 router-id in IP address format*]
5. **address-family ipv4 unicast**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router>` **`enable`**
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router#` **`configure terminal`**
		Enters global configuration mode.

Step 3	**`router ospfv3`** [*`process-id`*] **Example:** `Router (config)#` **`router ospfv3 4`**	Enables an OSPFv3 routing process to route IPv4 address-family traffic in IPv6 networks and enters router configuration mode.
Step 4	**`router-id`** [*`OSPFv3 router-id in IP address format`*] **Example:** `Router (config-rtr)#` **`Router-id 10.1.1.1`**	Identifies a specific router rather than allowing the dynamic assignment of the router ID to occur.

Step 5	**`address-family ipv4 unicast`**
	Example:
	`Router(config-rtr)#` **`address-family ipv4 unicast`**
		Places the router in address family configuration mode for IPv4 address family.

Step 6	**`exit`**
	Example:
	`Router (config-router-af)#` **`exit`**
		Exits global configuration mode and returns the router to privileged EXEC mode.

Working with Multiple Address Families

You can run Address Families OSPFv3 for IPv4 and IPv6 simultaneously on one interface.

Note To configure OSPFv3 for IPv4 and IPv6 simultaneously—with MANET and RAR features included, use tasks from this chapter and Chapter 10, "Configuring OSPFv3 for a MANET" The following example shows how to do this.

Example

```
version 15.1
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
ipv6 unicast-routing
!
subscriber authorization enable
!
subscriber profile Dargo7
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
!
no virtual-template subinterface
!
bba-group pppoe Group1
 virtual-template 1
 service profile Dargo7
!
interface Ethernet0/0
 no ip address
 pppoe enable group Group1
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Virtual-Template1
 no ip address
 ipv6 enable
 no peer default ip address
 no keepalive
!
interface vmi1
 ip address 64.1.1.1 255.255.255.0
 ipv6 enable
 ospfv3 6 network manet
 ospfv3 6 area 0 ipv6
 ospfv3 4 network manet
 ospfv3 4 area 0 ipv4
 physical-interface Ethernet0/0
!
ip forward-protocol nd
!
router ospfv3 4
 router-id 4.4.4.4
 log-adjacency-changes
 address-family ipv4 unicast
 exit-address-family
!
router ospfv3 6
 router-id 6.6.6.6
 log-adjacency-changes
 address-family ipv6 unicast
 exit-address-family
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Redistributing IPv4 Routes

Should you need to redistribute IPv4 routes between OSPFv3 Address Families and OSPFv2, be aware of common issues when redistributing IPv4 routes between OSPF processes as documented here: *http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080531fd2.shtml*

Example:
The following example shows how to redistribute IPv4 routes from OSPFv2 process 22 into OSPFv3 Address Families process 4:

```
Router (config)#router ospfv3 4
Router (config-router)#router-id 4.4.4.4
Router (config-router)#address-family ipv4 unicast
Router (config-router-af)#redistribute ?
  bgp        Border Gateway Protocol (BGP)
  connected  Connected
  eigrp      Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis       ISO IS-IS
  iso-igrp   IGRP for OSI networks
  lisp       Locator ID Separation Protocol (LISP)
  mobile     Mobile routes
  odr        On Demand stub Routes
  ospf       Open Shortest Path First (OSPF)
  ospfv3     OSPFv3
  rip        Routing Information Protocol (RIP)
  static     Static routes

Router (config-router-af)#redistribute ospf ?
  <1-65535>  Process ID

Router (config-router-af)#redistribute ospf 22 ?
  match        Redistribution of OSPF routes
  metric       Metric for redistributed routes
  metric-type  OSPF/IS-IS exterior metric type for redistributed routes
  route-map    Route map reference
  tag          Set tag for routes redistributed into OSPF
  vrf          VPN Routing/Forwarding Instance
  <cr>
```

```
Router (config-router-af)#redistribute ospf 22
```

Example:

The following example shows how to redistribute IPv4 routes from OSPFv3 Address Families process 4 into OSPFv2 process 22:

```
Router (config)#router ospf 22
Router (config-router)#redistribute ?
  bgp             Border Gateway Protocol (BGP)
  connected       Connected
  eigrp           Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis            ISO IS-IS
  iso-igrp        IGRP for OSI networks
  lisp            Locator ID Separation Protocol (LISP)
  maximum-prefix  Maximum number of prefixes redistributed to protocol
  mobile          Mobile routes
  odr             On Demand stub Routes
  ospf            Open Shortest Path First (OSPF)
  ospfv3          OSPFv3
  rip             Routing Information Protocol (RIP)
  static          Static routes

Router (config-router)#redistribute ospfv3 ?
  <1-65535>  Process ID

Router (config-router)#redistribute ospfv3 4 ?
  match        Redistribution of OSPF routes
  metric       Metric for redistributed routes
  metric-type  OSPF/IS-IS exterior metric type for redistributed routes
  nssa-only    Limit redistributed routes to NSSA areas
  route-map    Route map reference
  subnets      Consider subnets for redistribution into OSPF
  tag          Set tag for routes redistributed into OSPF
  <cr>

Router (config-router)#redistribute ospfv3 4 subnets ?
  match        Redistribution of OSPF routes
  metric       Metric for redistributed routes
  metric-type  OSPF/IS-IS exterior metric type for redistributed routes
  nssa-only    Limit redistributed routes to NSSA areas
  route-map    Route map reference
  tag          Set tag for routes redistributed into OSPF
  <cr>

Router (config-router)#redistribute ospfv3 4 subnets
```

Verifying OSPFv3 Address Families Configuration and Operation

You can use any combination of the commands listed in this section to check the operation status of OSPFv3 for Address Families.

Note You must be in privileged EXEC mode to enter the command listed in this section.

Command or Action	Purpose

`show run`
Example:
`Router# show run`
	Verify a configuration.

`show ospfv3`
Example:
`Router# show ospfv3`
	Displays general information about all OSPFv3 routing processes.

`show ospfv3 neighbor`
Example:
`Router# show ospfv3 neighbor`
	Displays OSPFv3 neighbor information per routing process.

`show ospfv3 neighbor detail`
Example:
`Router# show ospfv3 neighbor detail`
	Displays a detailed list of all neighbors.

show ospfv3 interface [*interface-type interface-number*] **Example:** `show ospfv3 interface e0/0`	Displays all OSPFv3 routing information for an interface.

The **show ospfv3** command can be used to show general information about the OSPFv3 Address Family router process.

```
Router# show ospfv3
 Routing Process "ospfv3 4" with ID 4.4.4.4
 Supports IPv4 Address Family
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Initial SPF schedule delay 1000 msecs
 Minimum hold time between two consecutive SPFs 2000 msecs
 Maximum wait time between two consecutive SPFs 2000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 Relay willingness value is 128
 Pushback timer value is 2000 msecs
 Relay acknowledgement timer value is 1000 msecs
 LSA cache Disabled : current count 0, maximum 1000
 ACK cache Disabled : current count 0, maximum 1000
 Selective Peering is not enabled
 Hello requests and responses will be sent multicast
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 1
        SPF algorithm executed 0 times
        Number of LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

Router# show ospfv3 neighbor

            OSPFv3 Router with ID (4.4.4.4) (Process ID 4)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/  -        00:00:19    3               Ethernet0/0

Router# show ospfv3 interface e0/0
Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE01:5500, Interface ID 3
  Area 0, Process ID 100, Instance ID 0, Router ID 4.4.4.4
  Network Type MANET, Cost: 10 (dynamic), Cost Hysteresis: Disabled
  Cost Weights: Throughput 100, Resources 100, Latency 100, L2-factor 100
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:01
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Incremental Hello is enabled
  Local SCS number 1
  Relaying enabled
```

CHAPTER 10

Configuring OSPFv3 for a MANET

This chapter provides the following major sections for configuring OSPFv3 in a Mobile Ad-hoc Network (MANET):

OSPFv3 for MANET

Configuring OSPFv3 for a MANET has similar requirements to many traditional OSPFv3 configurations. The primary difference is to configure the network type of OSPFv3 as a MANET. To optimize the use of OSPFv3 with MANETs, Cisco IOS implements extensions to OSPFv3 as defined in *IETF RFC 5820*. The result is a well-understood routing protocol designed for a constantly changing network topology constrained by limited bandwidth.

This is accomplished in several ways:

- Radio Aware Routing (RAR): Provides tight coupling of OSPFv3 with cooperative radios (fast convergence and re-convergence through neighbor-presence indicators). Determines accurate, real-time, link-metric costs.
- Incremental Hello: Minimizes OSPFv3 packet size.
- Caching Multicast Link-State Advertisements (LSAs): Minimizes OSPFv3 packet transmissions.
- Optimized Flooding (Overlapping Relay): Minimizes the number of flooded LSAs.
- Selective Peering: Reduces OSPFv3 network overhead by limiting redundant full-peering adjacencies.

Cooperative Radios

While non-cooperative radios are supported, OSPFv3 in a MANET operates best when used with cooperative radios, which is a configuration requiring Virtual Multipoint Interfaces (VMIs). See Chapter 5, "Introduction to Radio Aware Routing and MANET" for detailed procedures.

Note This document defines a Cooperative radio as a radio containing the firmware and software required to support RAR-based flows.

Initial Configuration Procedures

Configuring OSPFv3 for a MANET begins with the following tasks:

1. Enabling IPv6 Routing, page 10-2
2. Enabling IPv6 on the Interface, page 10-3
3. Configuring the OSPFv3 Process, page 10-4
4. Configuring the Interface for OSPFv3 MANETs, page 10-5

Enabling IPv6 Routing

This task enables IPv6 packet forwarding and IPv6 routing, both disabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose

Step 3	`ipv6 unicast-routing`
	Example:
	`Router(config)# ipv6 unicast-routing`
		Enables the forwarding of IPv6 unicast datagrams.

Step 4	`exit`
	Example:
	`Router(config)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Enabling IPv6 on the Interface

This task enables IPv6 on an interface—a prerequisite to configuring OSPFv3 on the interface. IPv6 is disabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ipv6 enable**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface [type number]`
	Example:
	`Router(config)# interface ethernet 0/0`
		Specifies an interface type and number and places the router in interface configuration mode.

	Command or Action	Purpose

Step 4	`ipv6 enable`
	Example:
	`Router(config-if)# ipv6 enable`
		Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Configuring the OSPFv3 Process

This task configures the OSPFv3 process for IPv6 or IPv4.

Note The commands in this task indicate IPv6. If you want to configure the OSPFv3 process for IPv4 instead, see the detailed steps for examples.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process*-id]
4. **router-id** [*OSPFv3 router-id in IP address format*]
5. **address-family ipv6 unicast**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	***router ospfv3*** [*process-id*] **Example:** `Router(config)#` **`router ospfv3 6`** **Example for IPv4:** `Router(config)#` **`router ospfv3 4`**	Enables OSPFv3 for IPv6 router configuration mode.
Step 4	**router-id** [*OSPFv3 router-id in IP address format*] **Example:** `Router(config-rtr)#` **`router-id 10.1.1.1`**	Enables the use of a fixed router ID.
Step 5	**address-family ipv6 unicast** **Example:** `Router(config-rtr)#` **`address-family ipv6 unicast`** **Example for IPv4:** `Router(config-rtr)#` **`address-family ipv4 unicast`**	Enables the address family for IPv6.
Step 6	**exit** **Example:** `Router(config-rtr)#` **`exit`**	Exits global configuration mode and returns the router to privileged EXEC mode.

Configuring the Interface for OSPFv3 MANETs

This configures the OSPFv3 process for IPv6 or IPv4.

Note The commands in this task indicate IPv6. If you want to configure the OSPFv3 process for IPv4 instead, see the detailed steps for examples.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ospfv3** [*process-id*] **area** *area-id* **ipv6 [instance** *instance-id*]
5. **ospfv3** [*process-id*] **network manet**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal**	Enters global configuration mode.
Step 3	**interface** [*type number*] **Example:** Router(config)# **interface vmi1**	Configures an interface type.
Step 4	**ospfv3** [*process-id*] **area** area-id **ipv6** [**instance** instance-id] **Example:** (Router-if)# **ospfv3 6 area 0 ipv6** **Example for IPv4:** (Router-if)# **ospfv3 6 area 0 ipv4**	Attaches the OSPFv3 process to an interface. **Note** The instance number defaults to 0 for ipv6.
Step 5	**ospfv3** [*process-id*] **network manet** **Example:** Router(config-if)# **ospfv3 6 network manet** **Example for IPv4:** Router(config-if)# **ospfv3 4 network manet**	Configures the OSPFv3 network type to MANET.
Step 6	**exit** **Example:** Router(config-if)# **exit**	Exits global configuration mode and returns the router to privileged EXEC mode.

EXAMPLE

```
version 15.1
!
hostname Router1
!
...
<output truncated>
...
interface Ethernet0/0
 no ip address
 ipv6 enable
 ospfv3 6 network manet
 ospfv3 6 area 0 ipv6
!
interface Ethernet0/1
 ip address 4.4.4.4 255.255.255.0
 ipv6 enable
 ospfv3 4 network manet
 ospfv3 4 area 0 ipv4
shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
!
router ospfv3 6
 router-id 1.1.1.1
 address-family ipv6 unicast
 log-adjacency-changes
!
router ospfv3 4
 router-id 4.4.4.4
 address-family ipv4 unicast
 log-adjacency-changes
...
<output truncated>
...
end
```

Radio Aware Routing in a MANET

This section describes how to configure OSPFv3 in MANETs for Radio Aware Routing (RAR).

Prerequisites

All radios in OSPFv3 for MANET must be cooperative radios attached to a Virtual Multipoint Interface (VMI).

Before performing the tasks in this section, you must configure OSPFv3 for MANETs on a VMI as described in Chapter 5, “Introduction to Radio Aware Routing and MANET”.

Link Metrics

Cooperative radios in the MANET report link-quality metrics, which can include the following information:

- Maximum Data Rate—the theoretical maximum data rate of the radio link, in bytes per second
- Current Data Rate—the current data rate achieved on the link, in bytes per second
- Latency—the transmission delay packets encounter, in milliseconds
- Resources—a percentage (0-100) that can represent the remaining amount of a resource (such as battery power)
- Relative Link Quality—a numeric value (0-100) representing relative quality, with 100 being the highest quality

Fine-Tuning RAR Configurations

You can fine-tune RAR configurations within a MANET by converting the link metrics to OSPFv3 link costs and configuring a hysteresis threshold. Configuring a hysteresis threshold on the resultant link costs helps minimize the propagation of LSAs responding to link-metric changes.

Metrics can be weighted during the configuration process to emphasize or de-emphasize particular characteristics. For example, if throughput is highly important, the metric for Current Data Rate (CDR) could be weighted more heavily into the composite metric. Similarly, a metric that is of no concern can be omitted.

Link metrics can change rapidly, often by very small degrees, which can result in a flood of meaningless routing updates. In a worst case scenario, the network will churn almost continuously as it struggles to react to minor variations in link quality. To alleviate this concern, Cisco provides a tunable dampening mechanism that allows the user to configure threshold values. Any metric change that falls below the threshold is ignored.

A tunable hysteresis mechanism allows users to adjust the threshold to the routing changes that occur when the router receives a signal that a new peer has been discovered, or that an existing peer is unreachable. The tunable metric is weighted and is adjusted dynamically to account for the following characteristics:

- Current and Maximum Bandwidth
- Latency
- Resources

- Hysteresis

Individual weights can be deconfigured and all weights cleared so that the cost is set back to the default value for the interface type. Based on the routing changes that occur, cost can be determined by the application of these metrics.

The dynamic cost metric used for interfaces is computed based on the Layer 2 (L2) feedback to Layer 3 (L3), where the metric calculations are as follows:

OC = maximum-data-rate
S1 = ospfv3 6 dynamic weight throughput (Bandwidth component)
S2 = ospfv3 6 dynamic weight resources (Resources component)
S3 = ospfv3 6 dynamic weight latency (Latency component)
S4 = ospfv3 6 dynamic weight L2 factor (L2 factor component)

Note While the commands and output in this section reflect IPv6 configurations, all examples and commands work for IPv4 as well.

Throughput = (current-data-rate)/(maximum-data-rate)

Router-dynamic cost = OC + (S1) + (S2) + (S3) + (S4)

For a dynamic cost to have the same cost as a default cost, all parameters must equal zero.

Each L2 feedback can contribute a cost in the range of 0 to 65535. To tune down this cost range, use the optional **weight** keyword in conjunction with the **throughput**, **resources**, **latency**, or **L2-factor** keyword. Each of these weights has a default value of 100 percent and can be configured in a range from 0 to 100. When 0 is configured for a specific weight, that weight does not contribute to the OSPFv3 cost.

Because cost components can change rapidly, you may need to dampen the amount of changes in order to reduce network-wide churn. Use the optional **hysteresis** keyword with the **threshold** *threshold-value* keyword and argument to set a cost change threshold. Any cost change below this threshold is ignored.

You can use the **hysteresis** keyword to specify a hysteresis value based on the percentage of change of the currently stored value in the routing table for the peer.

Each time the router receives a new PADQ packet from the radio for a peer, a new cost will be calculated for it. The **hysteresis** keyword specifies the amount of change required before saving the new value.

The hysteresis percent calculated is performed as follows:

If the absolute value of (new_cost - saved_cost) is greater than (hysteresis_percent*saved_cost), then the new_cost will be saved.

Because cost components can change rapidly, it might be necessary to dampen the volume of changes to reduce network-wide churn. The recommended values for S2, S3, and S4 are based on network simulations that may reduce the rate of network changes. The recommended value for S1 is zero to eliminate this variable from the route cost calculation.

While each network might have unique characteristics that require different settings to optimize actual network performance, these are recommended values intended as a starting point for optimizing a OSPFv3 network. Table 10-1 lists the recommended value settings for OSPFv3 cost metrics.

Table 10-1 Recommended Value Settings for OSPFv3 Cost Metrics

Setting	Metric Description	Default Value	Recommended Value
S1	ospfv3 6 dynamic weight throughout	100	0
S2	ospfv3 6 dynamic weight resources	100	29

Table 10-1 Recommended Value Settings for OSPFv3 Cost Metrics

Setting	Metric Description	Default Value	Recommended Value
S3	ospfv3 6 dynamic weight latency	100	29
S4	ospfv3 6 dynamic weight L2-factor	100	29

The overall link cost is computed using the following formula:

$$\text{LinkCost} = \text{OC} + \overset{\textcircled{1}}{\text{BW}}\left(\frac{\text{Throughput\_weight}}{100}\right) + \overset{\textcircled{2}}{\text{Resources}}\left(\frac{\text{Resources\_weight}}{100}\right) + \overset{\textcircled{3}}{\text{Latency}}\left(\frac{\text{Latency\_weight}}{100}\right) + \overset{\textcircled{4}}{\text{L2\_factor}}\left(\frac{\text{L2\_weight}}{100}\right)$$

$$\text{OC} = \left[\frac{(\text{ospf\_reference\_bw})}{(\text{MDR})(1000)}\right] \qquad \boxed{\text{ospf\_reference\_bw} = 10 \wedge 8}$$

$$\textcircled{1}\quad \text{BW} = \frac{(65535)\left(100 - \frac{\text{CDR}}{\text{MDR}}(100)\right)}{100}$$

$$\textcircled{2}\quad \text{Resources} = \frac{(100 - \text{resources})^3\,(65535)}{1000000}$$

$$\textcircled{3}\quad \text{Latency} = \text{latency}$$

$$\textcircled{4}\quad \text{L2\_factor} = \frac{(100 - \text{RLQ})(65535)}{100}$$

231048

EXAMPLE

To illustrate these settings, the following example shows how OSPFv3 cost metrics can be defined for a VMI interface with one type of radio:

```
interface vmi1
    ospfv3 6 cost dynamic hysteresis percent 10
    ospfv3 6 cost dynamic weight throughput 0
    ospfv3 6 cost dynamic weight resources 29
    ospfv3 6 cost dynamic weight latency 29
    ospfv3 6 cost dynamic weight L2-factor 29
```

EXAMPLE

The following is an IPv6 example of configuration:

```
version 15.1
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile pppoe_group_1
 pppoe service manet_radio
```

```
!
!
multilink bundle-name authenticated
!
no virtual-template subinterface
!
bba-group pppoe pppoe_group_1
 virtual-template 1
 service profile pppoe_group_1
!
interface Ethernet0/0
 no ip address
 shutdown
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Virtual-Template1
 no ip address
 ipv6 enable
 no peer default ip address
 no keepalive
!
interface vmi1
 no ip address
 ipv6 enable
 ospfv3 6 network manet
 ospfv3 6 area 0 ipv6
 physical-interface Ethernet0/0
!
ip forward-protocol nd
!
router ospfv3 6
 router-id 1.1.1.1
 log-adjacency-changes
 address-family ipv6 unicast
 exit-address-family
...
<output truncated>
...
end
```

Selective Peering for Efficiency

Use selective peering to minimize network costs by minimizing each node’s redundant adjacencies. For each OSPFv3 MANET node, you can restrict full-peering rights to the adjacent neighbors that enhance reachability while remaining cost-effective. For each neighbor adjacency calculated to cause excessive link costs, you can use selective peering to keep that neighbor in a 2-way state. This reduces the need for control-plane bandwidth by reducing database exchanges and routing updates.

Note Selective peering does not reduce dataplane connectivity. User traffic will flow over 2-way links when provided with the best path through the network.

Determining Peering Criteria

Upon discovery of each new neighbor within an OSPFv3 MANET node, selective peering determines whether the forming of an adjacency is cost-effective:

- Yes—Form the full-peering adjacency if the neighbor is not in the OSPFv3 link-state database or reachable via the Shortest Path Tree (SPT).
- No—Instead of forming a full-peering adjacency, maintain a 2-way state when the neighbor is in the OSPFv3 link-state database, reachable, and configured with a redundant-path threshold.

Because dynamic topologies can cause a neighbor path redunancy level to fall below the configured threshold, selective peering can change a neighbor 2-way state to full peering.

Link Costs

Selective peering includes link cost as a factor when determining adjacency formation. Ideally, only the links having the lowest costs are granted full-peering adjacency. You can configure OSPFv3 link costs manually, and with cooperative radio interfaces, link costs are obtained directly from the radios through the VMI.

Working with selective peering involves the following tasks:

- Enabling Selective Peering, page 10-12
- Preventing Full Peering over Poor Links, page 10-14
- Fine-Tuning Selective Peering, page 10-15

Enabling Selective Peering

This task explains how to enable OSPFv3 selective peering for IPv6 or IPv4.

Note The commands in this task indicate IPv6. If you want to configure the OSPFv3 process for IPv4 instead, see the detailed steps for examples.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast**
5. **manet peering selective** [redundancy <*level*>] [*per-interface*]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`router ospfv3 [process-id]`
	Example:
	`Router (config)# router ospfv3 6`
	Example for IPv4:
	`Router(config)# router ospfv3 4`
		Creates OSPFv3 process.

Step 4	`address-family ipv6 unicast`
	Example:
	`Router (config)# address-family ipv6 unicast`
	Example for IPv4:
	`Router(config)# address-family ipv4 unicast`
		Specifies that the OSPFv3 process supports the IPv6 unicast address family.

Step 5	`manet peering selective [redundancy <level>] [per-interface]`
	Example:
	`Router(config-rtr)# manet peering selective redundancy 2`
		Enables selective peering for all MANET interfaces using this router process.
		Optional: Redundancy level configuration (valid range 0-10). Lower redundancy reduces OSPFv3 control-plane overhead. Higher levels increase control-plane redundancy.
		1—Default redundancy level (maintains two or more paths—one primary and one redundant path) for each one-hop OSPFv3 neighbor.
		The per-interface option adjusts the scope of peer selection to the interface level.
		By default, the peer-selection scope is per-area and across all MANET interfaces in a given area.

Step 6	`exit`
	Example:
	`Router(config-rtr)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Preventing Full Peering over Poor Links

You can prevent full peering over poor links by performing this optional task, which configures the following:

- Configure OSPFv3 to wait for link metrics before considering a neighbor for OSPFv3 peering. (A cooperative radio may not advertise link metrics to the router before being discovered as a new OSPFv3 neighbor.)
- Configure OSPFv3 with a minimum metric threshold. If the radio-reported link metric is above this threshold, the neighbor will be held in 2-way state.

Note The commands in this task indicate IPv6. If you want to configure the OSPFv3 process for IPv4 instead, see the detailed steps for examples.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ospfv3** [*process-id*] **manet peering link-metrics** [<threshold>]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface [type number]`
	Example:
	`Router(config)# interface vmi1`
		Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose

Step 4	`ospfv3 [process-id] manet peering link-metrics [<threshold>]`
	Example:
	`Router(config-if)# ospfv3 6 manet peering link-metrics 200`
		Requires receipt of link metrics from each radio before considering the new neighbor for selective peering. If the threshold (0-65535) is specified, the resultant link cost must be less than the threshold. Otherwise, the neighbor remains in a 2-way state.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Fine-Tuning Selective Peering

This section describes how to optimize dynamic path costs by means of fine-tuning selective peering. Given a scenario without fine-tuning, each one-hop neighbor is awarded full-peering capabilities upon discovery, regardless of link cost:

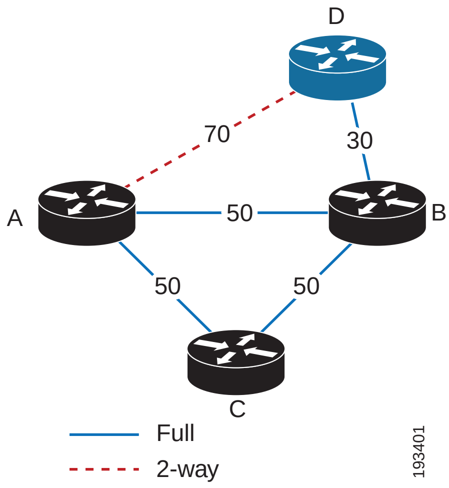
- Selective-peering redundancy level is greater than zero
- Link metrics are good (as determined by the configuration settings established in the "Preventing Full Peering over Poor Links" section on page 10-14)

As each additional neighbor is discovered, dynamic path costs are measurable immediately. To minimize path costs dynamically, you can configure the higher-cost links to remain in 2-way states until other peering opportunities become available.

Higher Costs without the Fine-Tuning

Consider the topology shown in Figure 10-1.

Figure 10-1 Peering Costs



Given the example shown in Figure 10-1, we have a static snapshot of a dynamic topology, beginning from this point:

- The redundancy level is set to 1 (the default value)—Router A attempts to maintain two paths for each one-hop neighbor.
- From the perspective of Router A, established neighbor sessions exist only with Routers B and C. Router D will join later.
- Router A has a full-peering relationship established with each of these known routers (B and C).
- The link cost for each of these neighbor sessions has a value of 50.
- At this point, only Router B has a link up to Router D—its peering relationship is full, and the link cost has a value of 30.

Change is then introduced between Router A and Router D:

1. Router D comes into radio range of Router A with a link cost of 70.
2. Router A establishes a full-peering relationship with this new neighbor. (The number of paths from Router A to Router D is currently 1 (through Router B).

The conclusion in this scenario (assigning full-peering capabilities between Routers A and D) is allowed given the original condition specified—the selective-peering redundancy level being greater than zero.

Improved Cost-Effectiveness through Fine-Tuning

To prevent the kind of scenario described in the "Higher Costs without the Fine-Tuning" section on page 10-15, you can fine-tune selective peering so that Routers A and D remain in a 2-way state until the link cost improves or an additional router comes into range—one with better link costs available to both routers (A and D).

Cost Thresholds for Redundant Paths

Setting a redundant-path cost threshold requires each redundant path to cost less than the existing, *best* path cost by a minimum value. For example, if the best link cost is 80, and you set the threshold value to 20, the new link cost must be less than 60 (80 minus 20).

Note The incremental improvement can be an absolute value or percentage.

Given the topology from Figure 10-1, if you set the redundant-path cost threshold to 20, you can prevent full peering between Routers A and D. This changes the outcome of our scenario, then, as follows:

1. Router D comes into radio range of Router A with a link cost of 70.
2. Selective peering compares link costs:
   - 80—Existing link cost between Routers A and D; the sum of link costs via Router B (50 + 30)
   - 70—The additional link cost between Routers A and D, if full peering is granted
3. The additional link cost (70) is incrementally better than the existing link cost (80) by a value of 10.
4. The incremental improvement (10) does not meet the minimum threshold (20); therefore, Routers A and D remain in the 2-way state.

Note The commands in this task indicate IPv6. If you want to configure the OSPFv3 process for IPv4 instead, see the detailed steps for examples.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ospfv3** [*process-id*] **manet peering cost** {threshold <*0-65535*> | percent <*0-100*>}
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface [type number]`
	Example:
	`Router(config)# interface vmi1`
		Configures an interface type.

Step 4	`ospfv3 [process-id] manet peering cost {threshold <0-65535> | percent <0-100>}`
	Example:
	`Router(config-if)# ospfv3 6 manet cost percent 10`
		Requires redundant paths to have an incrementally better path cost than the current best path cost. The incremental improvement can be specified either as an absolute value (0-65535) or as a percentage (0-100) of the current best path cost.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Verifying OSPFv3 MANET Configuration and Operation

You can use any combination of the commands listed in this section to check the operation status of OSPFv3 MANET for IPv6 or IPv4. See Appendix A, "Command Reference" for detailed command reference.

Note You must be in privileged EXEC mode to enter the command listed in this section.

Command or Action	Purpose
show run **Example:** `Router# show run`	Verify a configuration.

show ospfv3 [*process-id*]
Example:
`Router# show ospfv3 6`
Example for IPv4:
`Router# show ospfv3 4`
	Displays general information about all OSPFv3 routing processes.

show ospfv3 neighbor **Example:** `Router# show ospfv3 neighbor`	Displays OSPFv3 neighbor information per routing process.
show ospfv3 neighbor detail **Example:** `Router# show ospfv3 neighbor detail`	Displays a detailed list of all neighbors.
show ospfv3 neighbor manet **Example:** `Router# show ospfv3 neighbor manet`	Displays all neighbors in a MANET.

show ospfv3 [*process-id*] **interface** [interface-*type* *interface*-*number*]
Example:
`Router# show ospfv3 6 interface ethernet0/0`
Example for IPv4:
`Router# show ospfv3 4 interface ethernet0/0`
	Displays information about OSPFv3 routing processes for an interface.

EXAMPLES

The examples in this section show how you can use the **show ospfv3** command to display general information about the OSPFv3 router process.

Example:

```
Router# show ospfv3
 Routing Process "ospfv3 6" with ID 1.1.1.1
Supports IPv6 Address Family
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Initial SPF schedule delay 1000 msecs
 Minimum hold time between two consecutive SPFs 2000 msecs
 Maximum wait time between two consecutive SPFs 2000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 Relay willingness value is 128
 Pushback timer value is 2000 msecs
 Relay acknowledgement timer value is 1000 msecs
 LSA cache Disabled : current count 0, maximum 1000
 ACK cache Disabled : current count 0, maximum 1000
 Selective Peering is not enabled
 Hello requests and responses will be sent multicast
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 1
        SPF algorithm executed 0 times
        Number of LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Example:

```
Router# show ospfv3 neighbor

            OSPFv3 Router with ID (1.1.1.1) (Process ID 6)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/  -        00:00:19    3               Ethernet0/0
```

Example:

```
Router# show ospfv3 neighbor manet

            OSPFv3 Router with ID (1.1.1.1) (Process ID 6)

Area BACKBONE(0) (Inactive)
Codes: D - cost dynamic default, R - received link cost,
       I - inherited from interface

Neighbor ID       State  Nbr Relay    Cost        Interface
 2.2.2.2           FULL      -      10   (I)    Ethernet0/0
```

Example:

```
Router# show ospfv3 interface e0/0
Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE01:5500, Interface ID 3
  Area 0, Process ID 100, Instance ID 0, Router ID 1.1.1.1
  Network Type MANET, Cost: 10 (dynamic), Cost Hysteresis: Disabled
  Cost Weights: Throughput 100, Resources 100, Latency 100, L2-factor 100
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:01
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Incremental Hello is enabled
  Local SCS number 1
  Relaying enabled
```

CHAPTER 11

Configuring EIGRP in a MANET

This chapter explains how to configure the Enhanced Interior Gateway Routing Protocol (EIGRP) in a MANET.

This chapter includes the following major sections:

Understanding The Enhanced Interior Gateway Protocol

The Enhanced Interior Gateway Routing Protocol (EIGRP) integrates the capabilities of link-state protocols into distance vector protocols. EIGRP is distinguished from other routing protocols by the following key capabilities:

- Fast convergence
- Supports variable-length subnet mask
- Supports partial updates
- Supports multiple network layer protocols

A router running EIGRP stores all of its neighbors' routing tables so that the router running EIGRP can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbors to discover an alternate route. These queries propagate until an alternate route is found.

EIGRP supports variable-length subnet masks permitting routes to be automatically summarized on a network number boundary. EIGRP can be configured to summarize on any bit boundary at any interface.

EIGRP does not make periodic updates. EIGRP sends partial updates when the route metric changes. Propagation of partial updates is automatically bounded, so only routers needing the information update. EIGRP consumes significantly less bandwidth than the Interior Gateway Routing Protocol (IGRP).

Using EIGRP Cost Metrics for VMI Interfaces

When using EIGRP as the routing protocol, metrics allow EIGRP to respond to routing changes. The link-state metric is advertised as the link cost in the router link advertisement. The reply sent to any routing query always contains the latest metric information. The following exceptions result in an immediate update being sent:

- A down interface
- A down route
- Any change in metrics that result in the router selecting a new next hop

EIGRP receives dynamic raw radio link characteristics and computes a composite EIGRP metric based on a proprietary formula. To avoid churn in the network as a result of the change in the link characteristics, EIGRP uses a tunable dampening mechanism.

EIGRP uses the metric weights along with a set of vector metrics to compute the composite metric for local Routing Information Base (RIB) installation and route selections. The EIGRP composite metric is calculated using the formula:

metric = [K1 * BW + (K2 * BW) / (256 - Load) + K3 * Delay] * [K5 / (Reliability + K4)]

Note Use K values only after careful planning. Mismatched K values prevent a neighbor relationship from being built, which can cause your network to fail to converge.

Note If K5 = 0, the formula reduces to metric = [K1 * BW + (K2 * BW)/(256 - Load) + K3 * Delay].

Table 11-1 lists the EIGRP vector metrics and their descriptions.

Table 11-1 EIGRP Vector Metrics

Vector Metric	Description
BW	Minimum bandwidth of the route in kilobits per second. It can be 0 or any positive integer.
Delay	Route delay in tens of microseconds. It can be 0 or any positive number that is a multiple of 39.1 nanoseconds.
Reliability	Likelihood of successful packet transmission expressed as a number between 0 and 255. The value 255 means 100 percent reliability; 0 means no reliability.
Load	Effective load of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
MTU	Minimum Maximum Transmission Unit (MTU) size of the route in bytes. It can be 0 or any positive integer.

EIGRP monitors metric weights on an interface to allow for the tuning of EIGRP metric calculations and indicate Type of Service (ToS). Table 11-2 lists the K-values and their default.

Table 11-2 EIGRP K-Value Defaults

Setting	Default Value
K1	1
K2	0
K3	1
K4	0
K5	0

As shown in Table 11-2, cost configurations use the first two metrics—delay and bandwidth. The default formula of (BW +Delay) is the EIGRP metric. The bandwidth for the formula is scaled and inverted by the following formula:

(**10^7/minimum BW in kilobits per second**)

Note You can change the weights, but these weights must be the same on all the routers.

For example, look at an EIGRP link where the bandwidth to a particular destination is 128k and the Relative Link Quality (RLQ) is 50 percent.

BW = (256 * 10000000) / 128 = 20000000

Delay = (((10000000000 / 128) * 100) / (50 * 1000)) * 256 = (40000000 / 10) = 4000000

Using the cut-down formula, the EIGRP metric calculation would simplify to 256*(BW + Delay), resulting in the following value:

Metric = (BW + Delay) = 20000000 + 4000000 = 240000000

Understanding VMI Metric to EIGRP Metric Conversion

With the VMI interface, the quality of connection to a neighbor varies based on a number of characteristics computed dynamically as a result of layer 2 feedback to layer 3. Table 11-3 lists the metrics and their significance.

Table 11-3 MANET Metrics for VMI Interfaces

Metric	Format	Significance
current data rate	uint64_t	The current data rate reported from the radio. EIGRP converts the value into kilobits per second.
max data rate	uint64_t	The maximum data rate reported from the radio. EIGRP converts the value into kilobits per second.
latency	unsigned int	The latency computed and reported by the radio in milliseconds.
resources	unsigned int	The resources computed by the radio. A representation of resources, such as battery power, ranges from 0 to 100. If a radio does not report dynamic resources, the value is always 100.
relative link quality	unsigned int	An opaque number that ranges from 0 to 100 is computed by the radio, representing radio's view of link quality. 0 represents the worst possible link, 100 represents the best possible link.
link-load	unsigned int	An opaque number that ranges from 0 to 100 is computed by VMI, representing the load on the Ethernet link. 0 represents an idle Ethernet link, 100 represents a fully loaded Ethernet link. Note that this is not associated with the radio link.

Table 11-4 lists these EIGRP vector metric values map to the basic EIGRP interface parameters.

Note Although not explicit in Table 11-4, all variables are converted to the proper units.

Table 11-4 Mapping of MANET Metric Values to EIGRP Vector Metrics Values

Metric	EIGRP Metric	Mapping
current data rate	Bandwidth	Calculated: bandwidth = (256 * 10000000) / (current data rate / 1000)
relative link quality resources	Reliability	Calculated: reliability = (255 * (relative link quality) / 100)) * (resources / 100)
current data rate relative link quality	Delay	Calculated: delay = 256 * (1E10 / (current data rate / 1000)) * ((100 / relative link quality) / 1000) / 10
load	Load	Calculated: load = ((255 * link-load) / 100)

Understanding EIGRP Metric Dampening for VMI

Because metric components can change rapidly, the frequency of the changes have an impact on the network. Frequent changes require that prefixes learned though the VMI be updated and sent to all adjacencies. This update can result in further updates and, in a worst-case scenario, cause network-wide churn. To prevent such effects, metrics can be dampened, or thresholds set, so that any change that does not exceed the dampening threshold is ignored.

The following network changes cause an immediate update:

- A down interface
- A down route
- Any change in a metric that results in the router selecting a new next hop

Dampening the metric changes can be configured based on change or time intervals.

If the dampening method is change-based, changes in routes learned though a specific interface, or in the metrics for a specific interface, are not advertised to adjacencies until the computed metric changes from the last advertised value significantly enough to cause an update to be sent.

If the dampening method is interval-based, changes in routes learned though a specific interface, or in the metrics for a specific interface, are not advertised to adjacencies until the specified interval is met, unless the change results in a new route path selection.

When the timer expires, any routes with outstanding changes to report are sent out. If a route changes, such that the final metric of the route matches the last updated metric, no update is sent.

Understanding Neighbor Up/Down Signaling for EIGRP

MANETs are highly dynamic environments. Nodes may move in to, or out of, radio range at a fast pace. Each time a node joins or leaves, the network topology must be logically reconstructed by the routers. Routing protocols normally use timer-driven "hello" messages or neighbor time-outs to track topology changes. MANETs reliance on these mechanisms can result in unacceptably slow convergence.

This signaling capability provides faster network convergence by using link-status signals generated by the radio. The radio notifies the router each time a link to another neighbor is established or terminated by the creation and termination of PPPoE sessions. In the router, the EIGRP responds immediately to these signals by expediting the formation of a new adjacency (for a new neighbor) or tearing down an existing adjacency (if a neighbor is lost). For example, if a vehicle drives behind a building and loses its connection, the router immediately senses the loss and establishes a new route to the vehicle through neighbors that are not blocked. This high speed network convergence is essential for minimizing dropped voice calls and disruptions to video sessions.

When VMI with PPPoE is used and a partner node has left or a new one has joined, the radio informs the router immediately of the topology change. Upon receiving the signal, the router immediately declares the change and updates the routing tables.

The signaling capability offers the following benefits:

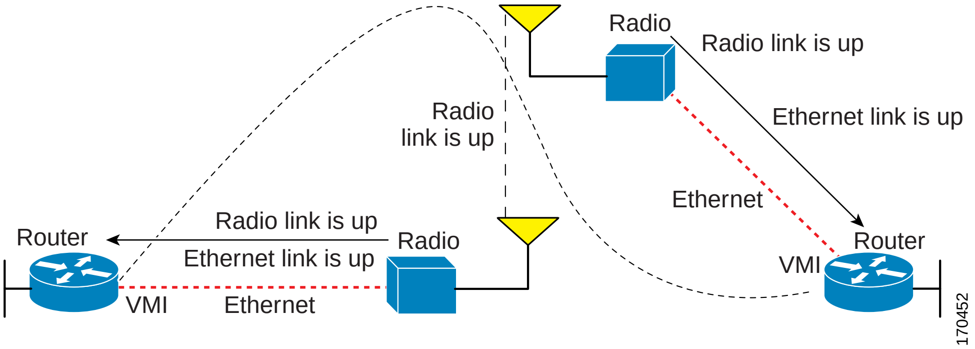
- Reduces routing delays and prevents applications from timing out
- Enables network-based applications and information to be delivered reliably and quickly over directional radio links
- Provides faster convergence and optimal route selection so that delay-sensitive traffic such as voice and video are not disrupted
- Reduces impact on radio equipment by minimizing the need for internal queuing/buffering
- Provides consistent Quality of Service (QoS) for networks with multiple radios

The messaging allows for flexible rerouting when necessary because of the following factors:

- Noise on the Radio links
- Fading of the Radio links
- Congestion of the Radio links
- Radio link power fade
- Utilization of the Radio

Figure 11-1 illustrates the signaling sequence that occurs when radio links go up and down.

Figure 11-1 Up and Down Signaling Sequence



Enabling EIGRP for IPv4

To create an EIGRP routing process, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **network** *network-number*
5. **end**

DETAILED STEPS

	Command	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`router(config)# router eigrp as-number`
	Example:
	`Router(config)# router eigrp 1`
		Enables an EIGRP routing process in global configuration mode.

Step 4	`router(config)# network network-number`
	Example:
	`Router(config)# network 10.2.2.0 0.0.0.255`
		Associates networks with an EIGRP routing process in router configuration mode.

Step 5	`End`
	Example:
	`Router(config-if)# end`
		Exits interface configuration.

Activating EIGRP IPv4 on a Configured VMI

Perform this task to activate EIGRP IPv4 on a configured VMI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vmi** *interface-number*
4. **no ip redirects**
5. **no ip split-horizon eigrp** *as-number*
6. **exit**
7. **router eigrp** *as-number*
8. **network** *network-number ip-mask*
9. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface` *`type interface-number`*
	Example:
	`Router(config-if)# interface vmi 1`
		Specifies the number of the VMI.

Step 4	`no ip redirect`
	Example:
	`Router(config)# no ip redirect`
		Disables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.

Step 5	`no ip split-horizon eigrp` *`as-number`*
	Example:
	`Router(config)# no ip split-horizon eigrp 1`
		Disables the split horizon mechanism for the specified session.

Step 6	`exit`
	Example:
	`Router(config-if)# exit`
		Exits a command mode to the next higher mode.

	Command or Action	Purpose
Step 7	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 1`	Enables EIGRP routing on the router and identifies the autonomous system number.
Step 8	**network** *network-number ip-mask* **Example:** `Router(config)# network 10.1.1.0 0.0.0.255`	Identifies the EIGRP network.

Step 9	**end**
	Example:
	`Router(config)# end`
		(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Enabling EIGRP for IPv6

Perform the following task to enable EIGRP for IPv6 on a specified interface. EIGRP for IPv6 is directly configured on the interfaces over which it runs, which allows EIGRP for IPv6 to be configured without the use of a global IPv6 address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface type number**
5. **ipv6 enable**
6. **ipv6 eigrp as-number**
7. **no shutdown**
8. **ipv6 router eigrp as-number**
9. **router-id** {*ip-address* | *ipv6-address*}
10. **no shutdown**
11. **end**

DETAILED STEPS

.

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal**	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** Router(config)# **ipv6 unicast-routing**	Enables IPv6 unicast routing.
Step 4	**interface** *type number* **Example:** Router(config)# **interface vmi1**	Creates a VMI.
Step 5	**ipv6 enable** **Example:** Router(config-if)# **ipv6 enable**	Enables IPv6 routing on the virtual template.
Step 6	**ipv6 eigrp** *as-number* **Example:** Router(config-if)# **ipv6 eigrp 100**	Enables EIGRP for IPv6 on a specified interface and specifies the Autonomous System (AS) number.
Step 7	**no shutdown** **Example:** Router(config-if)# **no shutdown**	Restarts a disabled interface or prevents the interface from being shut down.
Step 8	**ipv6 router eigrp** *as-number* **Example:** Router(config-if)# **ipv6 router eigrp 101**	Places the router in router configuration mode, creates an EIGRP routing process in IPv6, and allows you to enter additional commands to configure this process.
Step 9	**router-id** {*ip-address* | *ipv6-address*} **Example:** Router(config-router)# **router-id 10.1.1.1**	Enables the use of a fixed router ID.

	Command or Action	Purpose

Step 10	`no shutdown`
	Example:
	`Router(config-router)# no shutdown`
		Restarts a disabled EIGRP process or prevents the EIGRP process from being shut down.

Step 11	`end`
	Example:
	`Router(config-rtr)# end`
		(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Setting the EIGRP Metric Change-based Dampening for VMI

Perform the following tasks to set the change-based dampening interval for VMI:

This configuration assumes that a virtual template and appropriate PPPoE configurations have already been completed. Refer to the *Cisco IOS IP Mobility Configuration Guide* for VMI configuration details.

This configuration sets the threshold to 50 percent tolerance routing updates involving VMIs and peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **eigrp** *as-number* **interface** [**dampening-change** *value*] [**dampening-interval** *value*]
5. **physical-interface** *interface-type/slot*
6. **end**

DETAILED STEPS

	Command	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface type number`
	Example:
	`Router(config)# interface vmi 1`
		Enters interface configuration and creates a VMI.

	Command	Purpose
Step 4	**eigrp** *as-number* **interface** [**dampening-change** *value*] [**dampening-interval** *value*] **Example:** `Router(config-if)# eigrp 1 interface dampening-change 50`	Sets the EIGRP change-based dampening.
Step 5	**physical-interface** *interface-type/slot* **Example:** `Router(config-if)# physical-interface Ethernet0/0`	Creates a physical subinterface to be associated with the VMI.

Step 6	**end**
	Example:
	`Router(config-rtr)# end`
		(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Setting the EIGRP Interval-based Metric Dampening for VMI

Perform this task to set an interval-based dampening interval for VMI interfaces.

This configuration assumes that a virtual template and appropriate PPPoE configurations have already been completed. Refer to the *Cisco IOS IP Mobility Configuration Guide* for VMI configuration details.

This configuration sets the interval to 30 seconds at which updates occur for topology changes that affect VMI interfaces and peers:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **eigrp** *as-number* **interface** [**dampening-change** *value*] [**dampening-interval** *value*]
5. **end**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router>` **`enable`**
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router#` **`configure terminal`**
		Enters global configuration mode.

Step 3	**`interface`** *`type number`*
	Example:
	`Router(config)#` **`interface vmi 1`**
		Enters interface configuration and creates a VMI.

Step 4	**`eigrp`** *`as-number`* **`interface`** [**`dampening-change`** *`value`*] [**`dampening-interval`** *`value`*] **Example:** `Router(config-if)#` **`eigrp 1 interface dampening-interval 15`**	Sets the EIGRP interval-based dampening interval.

Step 5	**`End`**
	Example:
	`Router(config-if)#` **`end`**
		Exits interface configuration.

Examples

Basic VMI PPPoE Configuration with EIGRP IPv4

The following example illustrates the simplest configuration using EIGRP as the routing protocol. This configuration includes one VMI.

```
...
<output truncated>
...
!
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
!
!
multilink bundle-name authenticated
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe MANET1
 virtual-template 1
 service profile host1
!
```

```
!
interface FastEthernet0/0
 no ip address
 pppoe enable group MANET1
!
 interface Virtual-Template1
 ip unnumbered vmi1
 service-policy output FQ
!
interface vmi1
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 physical-interface FastEthernet0/0
!
router eigrp 1
 network 10.3.0.0 0.0.255.255
 auto-summary
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Basic VMI PPPoE Configuration Using EIGRP for IPv6

This example shows the basic requirements for configuring a VMI that uses EIGRP for IPv6 as the routing protocol. It includes one VMI.

```
...
<output truncated>
...
!
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
!
!
multilink bundle-name authenticated
!
policy-map FQ
 class class-default
  fair-queue
!
!
!
bba-group pppoe MANET1
 virtual-template 1
 service profile host1
!
!
interface FastEthernet0/0
 no ip address
 pppoe enable group MANET1
!
!
interface Virtual-Template1
 no ip address
 ipv6 unnumbered vmi1
 ipv6 enable
 service-policy output FQ
!
interface vmi1
 no ip address
 ipv6 address 2001:DB1:2::1/96
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 101
 no ipv6 split-horizon eigrp 101
 physical-interface FastEthernet0/0
!
ipv6 router eigrp 101
 router-id 10.9.1.1
 no shutdown
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

VMI PPPoE Configuration Using EIGRP for IPv4 and IPv6

The following examples shows the configuration VMI PPPoE using EIGRP as the IP routing protocol when you have both IPv4 and IPv6 addresses configured on the interface. This configuration includes one VMI. While EIGRP allows you to use the same AS number on an IPv4 EIGRP process and on an IPv6 process, we recommend using a unique AS number for each process for clarity.

```
...
<output truncated>
...
!
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe MANET1
 virtual-template 1
 service profile host1
!
!
interface FastEthernet0/0
 no ip address
 pppoe enable group MANET1
!
!
interface Virtual-Template1
 ip unnumbered vmi1
 ipv6 unnumbered vmi1
 ipv6 enable
 service-policy output FQ
!
```

```
interface vmi1
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip split-horizon eigrp 1
 ipv6 address 2001:0DB1:2::1/64
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 101
 no ipv6 split-horizon eigrp 1
 eigrp 1 interface dampening-interval 30
 eigrp 101 interface dampening-interval 30
 physical-interface FastEthernet0/0
!
router eigrp 1
 network 10.3.0.0 0.0.255.255
 auto-summary
!
!
ipv6 router eigrp 101
 router-id 10.9.1.1
 no shutdown
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

EIGRP Metric Dampening for VMI Interfaces

The **eigrp interface** command advertises routing changes for EIGRP traffic only.

The REPLY sent to any QUERY will always contain the latest metric information. The following exceptions result in an immediate UPDATE:

- A down interface
- A down route
- Any change in metric which results in the router selecting a new next hop

To prevent network-wide churn from frequent metric changes from impacting the network, even causing network-wide churn, metrics can be dampened, or thresholds set, so that any change that does not exceed the dampening threshold is ignored. The examples in this section show how to set the EIGRP dampening intervals to avoid such impacts.

EIGRP Change-based Metric Dampening for VMI Interfaces

The following example sets the threshold to 50 percent tolerance routing updates involving VMIs and peers:

```
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip split-horizon eigrp 1
 ipv6 address 2001:0DB1:2::1/64
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 101
 no ipv6 split-horizon eigrp 101
 eigrp 1 interface dampening-change 50
 eigrp 101 interface dampening-change 50
 physical-interface FastEthernet0/0
```

EIGRP Interval-based Metric Dampening for VMI Interfaces

The following example sets the interval to 30 seconds at which updates occur for topology changes that affect VMIs and peers:

```
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip split-horizon eigrp 1
 ipv6 address 2001:0DB1:2::1/64
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 101
 no ipv6 split-horizon eigrp 101
 eigrp 1 interface dampening-interval 30
 eigrp 101 interface dampening-interval 30
 physical-interface FastEthernet0/0
```

EIGRP VMI Bypass Mode

The following examples show the configuration of VMI bypass mode with EIGRP IPv4, EIGRP IPv6, and EIGRP for IPv4 and IPv6.

VMI Bypass mode PPPoE Configuration Using EIGRP for IPv6:

```
...
hostname host1
!
no ip domain lookup
!
ipv6 unicast-routing
!
ipv6 cef
!
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
multilink bundle-name authenticated
 no virtual-template subinterface
!
policy-map FQ
 class class-default
  fair-queue
!
!
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 load-interval 30
 ipv6 address 3514:1::1/64
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Virtual-Template1
 no ip address
 load-interval 30
 ipv6 address 3514:2::1/64
 ipv6 enable
 ipv6 eigrp 1
 no keepalive
 service-policy output FQ
!
interface vmi1
 no ip address
 load-interval 30
 ipv6 enable
 physical-interface FastEthernet0/0
 mode bypass
!
ipv6 router eigrp 1
 no shutdown
 redistribute connected
...
end
```

VMI Bypass mode PPPoE Configuration with EIGRP IPv4:

```
hostname host1
!
ip cef
!
no ip domain lookup
!
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
multilink bundle-name authenticated
!
no virtual-template subinterface
!
archive
 log config
!
policy-map FQ
 class class-default
  fair-queue
!
!
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 ip address 35.9.1.1 255.255.255.0
 load-interval 30
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Virtual-Template1
 ip address 4.3.3.1 255.255.255.0
 load-interval 30
 no keepalive
 service-policy output FQ
!
interface vmi1
 ! the IP Address of the vmi1 interface needs to be defined,
 ! but it will not be routable since the vmi interface will be
 ! down/down.
 ip address 4.3.9.1 255.255.255.0
 load-interval 30
 physical-interface FastEthernet0/0
 mode bypass
!
router eigrp 1
 redistribute connected
 network 4.2.0.0 0.0.255.255
 network 4.3.0.0 0.0.255.255
 auto-summary
!
...
end
```

VMI Bypass mode PPPoE Configuration Using EIGRP for IPv4 and IPv6:

```
...
hostname host1
!
ip cef
!
no ip domain lookup
!
ipv6 unicast-routing
!
ipv6 cef
!
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
multilink bundle-name authenticated
!
no virtual-template subinterface
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 ip address 35.9.1.1 255.255.255.0
 load-interval 30
 ipv6 address 3514:1::1/64
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Virtual-Template1
 ip address 4.3.3.1 255.255.255.0
 load-interval 30
 ipv6 address 3514:2::1/64
 ipv6 enable
 ipv6 eigrp 1
 no keepalive
 service-policy output FQ
!
interface vmi1
 ip address 4.3.9.1 255.255.255.0
 load-interval 30
 ipv6 enable
 physical-interface FastEthernet0/0
 mode bypass
!
router eigrp 1
 redistribute connected
 network 4.2.0.0 0.0.255.255
 network 4.3.0.0 0.0.255.255
 auto-summary
!
ipv6 router eigrp 1
 eigrp router-id 35.9.1.1
 no shutdown
 redistribute connected
...
end
```

CHAPTER 12

Understanding and Configuring IP Multiplexing

This chapter discusses IP multiplexing for satellite topologies in the following major sections:

Understanding IP Multiplexing

You can use IP multiplexing to optimize IPv4 and IPv6 traffic in environments where packet-per second transmission limitations cause inefficient bandwidth utilization, such as a satellite network. IP multiplexing addresses this constraint by bundling smaller packets into one larger UDP packet, known as a superframe. The router then sends the superframe to the destination router which demultiplexes the individual packets out of the superframe and routes them to their final destination.

IP multiplexing uses Cisco IOS access control lists (ACLs) to identify outbound packets. You can configure standard, extended, or named ACLs to use with IP multiplexing. IP multiplexing maintains a the cache of recent ACL lookup results to optimize traffic classification.

The following interface types support IP multiplexing:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- IPv4 GRE tunnel
- IPv6 GRE tunnel
- Ethernet, Fast Ethernet, and Gigabit Ethernet VLAN
- VMI over Ethernet, Fast Ethernet, and Gigabit Ethernet
- Virtual-Template on VMI

Both endpoints of the multiplex connection must be configured for multiplexing with corresponding source and destination addresses. If a superframe arrives at an interface with IP multiplexing not configured or not configured to receive superframes from the destination router, the superframe is not demultiplexed, and the superframe is routed normally. If IP multiplexing is not configured, then outbound packets are routed normally.

Configuring IP Multiplexing

When configuring IP multiplexing, you must configure each device before enabling the configuration. Failure to do so will result in lost packets at the end that is not yet configured.

Configuring IP multiplexing requires the following procedures:

- Configuring ACLs to Identify Traffic, page 12-2
- Configuring an IP Multiplex Profile, page 12-2
- Configuring IP Multiplexing on an Interface, page 12-6

The following procedures are optional and can be used to optimized IP multiplexing:

- Configuring the Multiplex Lookup Cache Size, page 12-8
- Configuring IP Multiplexing on an Interface, page 12-6

Configuring ACLs to Identify Traffic

IP multiplexing uses ACL definitions to identify traffic selected for multiplexing treatment. You can configure standard, extended or named ACLs to define traffic you want to multiplex. Packets that are not identified by an ACL used for multiplexing are routed normally.

Refer to the following URL on Access Control Lists for more information on how to configure an ACL: http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_acc_list_ov_ps10591_TSD_Products_Configuration_Guide-Chapter.html.

In general, an ACL statement for IP multiplexing should have the following format:

```
permit udp any host destination_IP_address UDP_port_number
```

IP Multiplexing makes caching decisions based on destination IP address, destination port, and protocol type. Although ACLs can be defined to filter packets based on other attrbutes, using other attributes in an IP Multiplexing ACL may have unexpected and/or unwanted results.

Configuring an IP Multiplex Profile

The attributes associated with an IP multiplexing connection between two routers are configured in an IP multiplex profile.

Tip You must configure an IP multiplex profile for each endpoint of an IP multiplex connection in the network.

You must define the following information for an IP multiplex profile:

- Profile name
- Access control list (ACL) used to classify outbound IP packets as IP multiplex traffic
- Source and destination IP addresses to be included in the superframe header
- Maximum amount of time the router waits to fill a superframe before sending a partial superframe

You can define the following optional information for an IP multiplex profile:

- Maximum size of an outbound IP packet to be considered for multiplexing
- Maximum MTU size of a superframe
- TTL value to be included in the superframe IP header

Perform the following task to configure an IP multiplex profile.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. {**ip** | **ipv6**} **mux profile** *profile_name*
4. **access-list** *access-list name or number*
5. **source** {*ip_address* | *interface name*}
6. **destination** *ip_address*
7. **(Optional) holdtime** *milliseconds*
8. **(Optional) maxlength** *bytes*
9. (Optional) mtu *bytes*
10. **(Optional) ttl** *hops*
11. (Optional) **no singlepacket**
12. **no shutdown**
13. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router>` **`enable`**
	`Router#`
		Enables privileged EXEC mode.
		Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router#` **`configure terminal`**
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	{**`ip`** | **`ipv6`**} **`mux profile`** *`profile_name`*
	Example:
	`Router(config)#`**`ip mux profile routeRTP-SJ`**
	`Router(config-ipmux-profile)#`
		Creates an IP multiplex profile with the specified name and enters IP multiplexing mode profile mode.
		Use the **ip** keyword to create an IPv4 profile. Use the **ipv6** keyword create an IPv6 profile.

Step 4	**`access-list`** *`access-list name or number`*
	Example:
	`Router(config-ipmux-profile)#`
	`access-list routeRTP-SJ`
	`Router(config-ipmux-profile)#`
		Applies the specified access list to the profile and uses the statements in the access list to identify outbound traffic for multiplexing.

Step 5	**`source`** {*`ip_address`* | `interface` *`interface-type`*}
	Example:
	`Router(config-ipmux-profile)#`**`source 172.16.1.1`**
	`Router(config-ipmux-profile)#`
		Designates the source IP address for the profile. The source address is the IP address assigned to the outbound interface. If you created an IPv4 profile, then use an IPv4 address. If you created an IPv6 profile, then use an IPv4 address.
		If you use the **interface** keyword, IP multiplexing will use the IP address configured for that interface. Beware if you are using the **interface** keyword for an IPv6 interface with multiple IP addresses assigned to it. IP multiplexing may not use the IP address you want for multiplexing.
		The profile must be shutdown in order to change the source address.
		Note This source address must be configured as the destination address in the corresponding profile at the other end of the IP multiplexing connection.

	Command or Action	Purpose

Step 6	**`destination`** *`ip_address`*
	Example:
	`Router(config-ipmux-profile)#`
	`destination 172.172.16.2.1`
	`Router(config-ipmux-profile)#`
		Designates the IP address to which superframes will be sent from the particular profile. The destination address must match the source address of the corresponding profile on the destination router. If you created an IPv4 profile, then use an IPv4 address. If you created an IPv6 profile, then use an IPv6 address.
		The profile must be shutdown in order to change the destination address.
		Note This destination address must be configured as the source address in the corresponding profile at the other end of the IP multiplexing connection.

Step 7	**`holdtime`** *`milliseconds`*
	Example:
	`Router(config-ipmux-profile)#`
	`holdtime 150`
	`Router(config-ipmux-profile)#`
		(Optional) Configures the amount of time in milliseconds that a multiplex profile waits to fill the superframe before sending a partial superframe.
		Valid values range from 20 to 250 milliseconds
		If you do not set a hold time, the profile uses 20 milliseconds as a default

Step 8	**`maxlength`** *`bytes`*
	Example:
	`Router(config-ipmux-profile)#`
	`maxlength 128`
	`Router(config-ipmux-profile)#`
		(Optional) Configures the largest packet size that the multiplex profile can hold for multiplexing. A larger packet size will not be multiplexed even if it correctly matches the ACL attached to the profile.
		Valid values range from 64 to 1472 bytes.
		If you do not configure a maximum packet length, then any packet that fits into the superframe is multiplexed.

Step 9	**`mtu`** *`bytes`*
	Example:
	`Router(config-ipmux-profile)#`
	`maxlength 512`
	`Router(config-ipmux-profile)#`
		(Optional) Configures the maximum size for the outbound superframe.Valid values range from 256 to 1500 bytes.
		If you do not configure a MTU values, the profile uses 1500 bytes as a default.
		The superframe size specified in the **mtu** command includes the IP and UPD headers for the superframe of 48 bytes for IPv6 and 28 bytes for IPv4 packets. Therefore an IPv6 mtu configured to 1400 bytes will accept 1352 bytes of data before sending a full superframe. An IPv4 mtu configured to 1400 bytes will accept 1372 bytes of data before sending a full superframe.

Step 10	**`ttl`** *`hops`*
	Example:
	`Router(config-ipmux-profile)#`**`ttl 128`**
	`Router(config-ipmux-profile)#`
		(Optional) Configures the superframe time-to-live (ttl) for the IP header of the superframe.
		Valid values range from 1 to 255 hops.
		By default, the ttl value is set to 64 hops.

	Command or Action	Purpose

Step 11	`singlepacket`
	Example:
	`Router(config-ipmux-profile)#`
	`singlepacket`
	`Router(config-ipmux-profile)#`
		Configures the router to send the original packet unmodified if there is only one packet to multiplex when the hold timer expires.
		By default, single packets are multiplexed into superframes when the hold timer expires.

Step 12	`no shutdown`
	Example:
	`Router(config-ipmux-profile)#`**`no`**
	`shutdown`
	`Router(config-ipmux-profile)#`
		Activates the multiplex profile
		If you want to change the ACL associated with the profile or the contents of the ACL, you must enter the **shutdown** command for the profile, make the changes and then enter the **no shutdown** command.

Step 13	`exit`
	Example:
	`Router(config-ipmux-profile)#`**`exit`**
	`Router(config)#`
		Exits the configuration mode and returns to global configuration mode.

Configuring IP Multiplexing on an Interface

IP multiplexing must be configured on an interface and the interface enabled to activate IP multiplexing. Once IP multiplexing is configured on an interface, all multiplex profiles are used to classify IP packets routed for transmission on the interface. The following Cisco IOS interfaces support IP Multiplexing:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- IPv4 GRE tunnel
- IPv6 GRE tunnel
- Ethernet, Fast Ethernet, and Gigabit Ethernet VLAN
- VMI over Ethernet, Fast Ethernet, and Gigabit Ethernet
- Virtual-Template on VMI

Perform the following procedure to enable IP multiplexing on an interface:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type/slot*
4. {**ip** | **ipv6**} **mux**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable** Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enters global configuration mode.
Step 3	**interface** *type/slot* **Example:** Router(config)# **interface fastethernet0/1** Router(config-if)#	Enters interface configuration mode for the specified interface.
Step 4	{**ip** | **ipv6**} **mux** **Example:** Router(config-if)#**ipv6 mux** Router(config-if)#	Enables IP multiplexing on the interface. Use **ip mux** for an IPv4 interface and **ipv6 mux** for an IPv6 interface. **Note** You can use the **show interface** command to verify that the interface is administratively up and whether the interface has an IPv4 or IPv6 address configured for the interface.
Step 5	**exit** **Example:** Router(config-ipmux-policy)#**exit** Router(config)#	Exits IP multiplex policy mode.

Configuring UDP Port for Superframe Traffic

The receiving router identifies incoming superframes by destination IP address, protocol type (UDP), and a UDP port number. A single UDP port number is used for all IP multiplexing traffic in the network.

Note If you do not configure a UDP port for IP multiplexing traffic, the system uses the default value of 6682. This value is inserted in the UDP header of the outbound superframe. If you use the default UDP port value, make sure that all routers sending or receiving IP multiplexing traffic use the same value.

Perform this task to configure the UDP port for IP multiplexing traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. {**ip** | **ipv6**} **mux udpport** *port_number*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> `**`enable`**
	`Router#`
		Enables privileged EXEC mode.
		Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	{**`ip`** | **`ipv6`**} **`mux udpport`** *`port_number`*
	Example:
	`Router(config)#ip mux udpport 5000`
	`Router(config)#`
		Configures the UDP port for IP multiplexing.
		Valid Values range from 1024 to 49151.

Configuring the Multiplex Lookup Cache Size

The lookup cache maps the destination address, protocol type, and port number to a multiplex profile to reduce performance overhead related to ACL lookups. You can configure the maximum size of the cache to manage memory utilization on the router.

The maximum size of the IPv6 cache can range from 1,000,000 to 4,294,967,295 bytes which corresponds to 10,419 to 44,739,242 entries. The maximum size of the IPv4 cache can range from 1,000,000 to 4,294,967,295 bytes which corresponds to 11,363 to 49,367,440 entries.

Note If you do not configure the cache size, the cache size defaults to 1,000,000 bytes, which will hold 11,363 entries for IPv4 multiplex and 10,419 for IPv6 multiplex.

Perform this task to configure the size of the lookup cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ip mux cache** *size*

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode.
		Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	`ip mux cache` *size*
	Example:
	`Router(config)#ip mux cache 5000000`
	`Router(config)#`
		Configures the size of the IP multiplexing look cache.
		Valid Values range from 1000000 to 4294967295 bytes.

Configuring the IP Multiplex Policy

An IP multiplex policy is used to retain DSCP priorities of the underlying data traffic. An IP multiplex policy approximates QoS. If you configure an IP multiplex policy, then you can configure DSCP values for the superframe header and you can specify that only the packets with a specified DSCP value be placed into the superframe. Note that a policy can match more than one DSCP value.

A router may have up to three multiplex policies for IPv6 and three multiplex policies for IPv4 defined on it. Multiplex policies are global and apply to all multiplex profiles on a router.

If the DSCP value assigned to a packet does not match any multiplex policy, then the router uses the default multiplex policy for superframe multiplexing. Superframes for the default policy have a DSCP value set to 0.

If you do not configure an IP multiplex policy, then all IP multiplex packets are sent using the default IP multiplex policy with a DSCP value equal to 0.

The DSCP values in each packet header remains intact as the packet goes through the multiplexing and demultiplexing processes.

Configuring DSCP Value for Outbound Superframes

Perform this task to create a multiplex policy, specify the matching DSCP values for a superframe, and specify the outbound DSCP value for the header of the superframe.

If you do not configure a DSCP value for an outbound superframe, superframes are sent with DSCP equal to 0.

If the DSCP value for packets selected for multiplexing does not match any multiplex policy **matchdscp** values, then these packets are sent using the default multiplex policy which has a DSCP set to 0.

A packet found to match the **matchdscp** value is put in the superframe with the corresponding multiplex policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. {**ip** | **ipv6**} **mux policy** *policy_name*
4. **outdscp** *DSCP_value*
5. **matchdscp** *DSCP_value*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode.
		Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	`{ip	ipv6} mux policy policy-name`
		Example:
		`Router(config)#ip mux policy RouteRTP-SJ`
		`Router(config-ipmux-policy)#`
			Configures an IP policy with the specified name and enters IP multiplex policy configuration mode.

	Command or Action	Purpose

Step 4	**`outdscp`** *`DSCP_value`*
	Example:
	`Router(config-ipmux-policy)#`
	`outdscp 10`
	`Router(config-ipmux-policy)#`
		Configures the DSCP value for the outbound superframe.
		Valid values range from 0 to 63. The following DSCP values are also valid:
		af11 Match packets with AF11 dscp (001010)
		af12 Match packets with AF12 dscp (001100)
		af13 Match packets with AF13 dscp (001110)
		af21 Match packets with AF21 dscp (010010)
		af22 Match packets with AF22 dscp (010100)
		af23 Match packets with AF23 dscp (010110)
		af31 Match packets with AF31 dscp (011010)
		af32 Match packets with AF32 dscp (011100)
		af33 Match packets with AF33 dscp (011110)
		af41 Match packets with AF41 dscp (100010)
		af42 Match packets with AF42 dscp (100100)
		af43 Match packets with AF43 dscp (100110)
		cs1 Match packets with CS1(precedence 1) dscp (001000)
		cs2 Match packets with CS2(precedence 2) dscp (010000)
		cs3 Match packets with CS3(precedence 3) dscp (011000)
		cs4 Match packets with CS4(precedence 4) dscp (100000)
		cs5 Match packets with CS5(precedence 5) dscp (101000)
		cs6 Match packets with CS6(precedence 6) dscp (110000)
		cs7 Match packets with CS7(precedence 7) dscp (111000)
		default Match packets with default dscp (000000)
		ef Match packets with EF dscp (101110)

	Command or Action	Purpose
Step 5	**matchdscp** *DSCP_value* **Example:** Router(config-ipmux-policy)# **matchdscp 45** Router(config-ipmux-policy)#	Configures the DSCP value that IP multiplexing uses to compare against the DSCP value in packets bound for multiplexing. A match puts the packet in the superframe that corresponds to the IP multiplex policy. You can enter more than one value. Valid values range from 0 to 63. The following DSCP values are also valid: af11 Match packets with AF11 dscp (001010) af12 Match packets with AF12 dscp (001100) af13 Match packets with AF13 dscp (001110) af21 Match packets with AF21 dscp (010010) af22 Match packets with AF22 dscp (010100) af23 Match packets with AF23 dscp (010110) af31 Match packets with AF31 dscp (011010) af32 Match packets with AF32 dscp (011100) af33 Match packets with AF33 dscp (011110) af41 Match packets with AF41 dscp (100010) af42 Match packets with AF42 dscp (100100) af43 Match packets with AF43 dscp (100110) cs1 Match packets with CS1(precedence 1) dscp (001000) cs2 Match packets with CS2(precedence 2) dscp (010000) cs3 Match packets with CS3(precedence 3) dscp (011000) cs4 Match packets with CS4(precedence 4) dscp (100000) cs5 Match packets with CS5(precedence 5) dscp (101000) cs6 Match packets with CS6(precedence 6) dscp (110000) cs7 Match packets with CS7(precedence 7) dscp (111000) default Match packets with default dscp (000000) ef Match packets with EF dscp (101110)
Step 6	**exit** **Example:** Router(config-ipmux-policy)#**exit** Router(config)#	Exits IP multiplex policy mode.

Verifying the IP Multiplexing Configuration

The following procedures can be used for verifying the IP Multiplexing configuration on the router:

Displaying IP Multiplex Statistics, page 12-13

Displaying IP Multiplexing Cache Statistics, page 12-13

Displaying IP Multiplex Profiles, page 12-13

Displaying IP Multiplexing Statistics for an Interface, page 12-14

Displaying IP Multiplex Statistics

You can use the **show** {**ip** | **ipv6**} **mux** command to display IP multiplexing statistics.

The following example shows how to display IPv4 multiplex statistics:

```
router#show ip mux
Superframe UDP Port: 6682

Multiplex Policies
muxpol             Outbound DSCP:       19
                    Match DSCP values:   af21 19
 muxpol2            Outbound DSCP:       af11
                    Match DSCP values:   11
 muxpol3            Outbound DSCP:       2
                    Match DSCP values:   1

IPv4 Multiplex Cache Statistics
  Current Entries:                3
  Maximum Number of Entries:      56818
  Cache High Water Mark:          3
  Total Stale Entries:            0
  Total Do-Not-Multiplex Entries: 0

router#
```

Displaying IP Multiplexing Cache Statistics

You can use the **show** {**ip** | **ipv6**} **mux cache** command to display IP multiplexing cache statistics.

The following example shows how to display the cache statistics:

```
router#show ip mux cache

IPv4 Multiplex Cache Statistics
  Current Entries:                3
  Maximum Number of Entries:      56818
  Cache High Water Mark:          3
  Total Stale Entries:            0
  Total Do-Not-Multiplex Entries: 0

IPv4 Multiplex Cache Contents
Destination Address   Port      Protocol    Profile
----------------------------------------------------
20.20.20.24          0         UDP         r1
20.20.20.20          1000       UDP        r1
20.20.20.21          1000      UDP         r1
router#
```

Displaying IP Multiplex Profiles

You can use the **show** {**ip** | **ipv6**} **mux profile** command to display IP multiplex profile statistics. If you do not enter a profile name, this command displays statistics for all multiplex profiles.

The following example shows how to display the profile statistics for the IPv6 profile r1v6:

```
router#show ipv6 mux profile
Profile r1v6
 Shutdown:                   No
 Destination:                2000:0:1:2:A8BB:CCFF:FE01:5610
 Source:                     2000:0:1:2:A8BB:CCFF:FE01:5510
 Access-list:                muxv6acl
 TTL:                        64
  Max mux length:            1452
 MTU:                        1500
  Hold time(ms):             20
  Single packet superframes: Enabled

  Inbound (demux) Statistics
   Superframes received:         0
   Packets demultiplexed:        0
   Avg. Inbound Multiplex ratio: N/A

Outbound (mux) Statistics
  Default Policy
   Packets: 40825  Full Superframes: 0       Partial Superframes: 20293
   Avg. Outbound   Multiplex ratio:  2.1:1   Mux length exceeded: 0

  Policy policy1
   Packets: 1273   Full Superframes: 0       Partial Superframes: 532
   Avg. Outbound Multiplex ratio:    2.39:1  Mux length exceeded: 0

router#
```

Displaying IP Multiplexing Statistics for an Interface

You can use the **show** {**ip** | **ipv6**} **mux interface** command to display IP multiplexing statistics for a specific interface.

If you do not specify a specific interface, this command displays statistics for all interfaces with IP multiplexing configured.

The following example shows how to display IP multiplex statistics for Ethernet 0/1:

```
router#show ip mux interface Ethernet0/1
IPv4 Multiplexing statistics for Ethernet0/1
  Transmit
   IPv4 superframes transmitted: 20430
   IPv4 packets multiplexed:     30555
   Average TX mux ratio:         1.49:1
  Receive
   IPv4 super frames received:   22009
   IPv4 packets demuxed:         32634
   IPv4 superframes rejected:    0
   IPv4 format errors:           0
   Average RX mux ratio:         1.48:1
router#
```

CHAPTER 13

Zeroization

Zeroization consists of erasing any and all potentially sensitive information in the router. This includes erasure of main memory, cache memories, and other memories containing packet data, NVRAM, and selected files in the Flash file system such as crash dumps. Zeroization is launched upon the initiation of a user command and subsequent trigger. In this document declassification and zeroization mean the same thing, and they are used interchangeably.

Note Zeroization is available on only the Cisco 5930 ESR.

Restrictions for Zeroization

The following restrictions apply when using zeroization on the Cisco 5930 ESR.

- When zeroization is enabled do not use the auxiliary (AUX) port for any function other than an actuator, such as a push button. There is no way to reliably ascertain whether a device connected to the AUX port might trigger zeroization. We recommend that if zeroization is enabled, no devices, with the exception of the zeroization actuator, be attached to the AUX port. There are some AUX port configuration restrictions that apply when zeroization is enabled.
- Zeroization can only be invoked and executed locally. It cannot be invoked and executed remotely through a Telnet session. Zeroization takes about five miutes to complete.
- Zeroization shuts down all network interfaces and causes zeroization of the Cisco IOS configuration and object code files, including all IP addresses on the router contained in volatile memory.

Scrubbing the Router Memory

Scrubbing is defined as performing several passes through the memory areas, overwriting the memory using a separate data pattern for each pass. The data patterns used for scrubbing consist of separate passes; each pass fills the memory with the following data patterns:

- All ones (that is, 0xffff ffff)
- Alternating ones and zeroes (that is, 0xa5a5 a5a5)
- Alternating zeroes and ones (that is, 0x5a5a 5a5a)
- All zeroes (that is, 0x0000 0000)

The data patterns ensure that

- Each bit in the memory is cleared to zero and set to one at least once.
- The final state of the memory is such that all prior information is erased.

The following items in the router memory are scrubbed:

- Dual-port RAM in the CPM
- Main memory

All the main memory is scrubbed except the memory area containing a small program loop that does the actual scrubbing.

The following items in the router memory cannot be scrubbed:

- Console and AUX port UART FIFO queues. A series of characters is forced through the FIFO queues to ensure that all sensitive information in the FIFO queues is flushed.
- NVRAM, which is erased entirely.
- Flash memory file system, which is erased entirely.

Zeroization Command Reference 3

- Caches, which are flushed and invalidated, eliminating all of the information. The process of scrubbing the main memory causes all cache lines to receive the scrubbing data patterns.

Note Some items cannot be completely scrubbed. For example, some devices provide a reset or invalidate their memory, rather than providing a full data path through which the scrubbing patterns can be written upon memory.

End User Interface

The following Zeroization (declassification) commands are supported on the Cisco 5930 ESR in Cisco IOS Release 15.2(4)GC.

- service declassify, page A-69

For information about these commands, see *Appendix A, "Command Reference"*

APPENDIX A

Command Reference

This appendix provides command reference documentation in the following major sections:

- Debug Commands
- List of Commands, page A-1
- Commands, page A-4

Debug Commands

You can search for **debug** commands from privileged EXEC mode.

Caution Do not use debug commands unless a Cisco Support engineer instructs you to do so.

Example for DLEP

This example shows how to display **debug** commands for Dynamic Link Exchange Protocol (DLEP):

```
router# debug dlep ?
   client    debug DLEP client information
   neighbor  DLEP neighbor transaction information
   server    DLEP server transaction information
   timer     display DLEP timer information
```

List of Commands

This section lists the mobility commands modified or introduced in this Configuration Guide:

- access-list, page A-5
- clear dlep client, page A-6
- clear dlep counters, page A-7
- clear dlep neighbor, page A-8
- clear ospfv3, page A-9
- clear pppoe relay context, page A-11
- clear vmi counters, page A-12
- destination, page A-13

Commands

The following section provides the complete reference pages for all commands listed in this appendix.

access-list

To assign an existing access list to the IP multiplex profile, enter the **access-list** command. To clear the access list associated with the IP multiplex profile, use the **no** form of the command.

access-list {{1-199} |{1300-2699} | *name*}

[**no**] **access-list**

Syntax Description

1-199	Standard access list number to use with the IP multiplex profile.
1300-2699	Extended access list number to use with the IP multiplex profile.
name	IPv6 access list name to use with the IP multiplex profile.

Command Modes

IP multiplexing profile configuration (config-ipmux-profile)

IPv6 multiplexing profile configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

You must configure an access list for IP multiplexing to work. The access list identifies the traffic to be considered for multiplexing. If you do not configure an access list, then no packets are queued for multiplexing.

If you enter the **access-list** command again, then the new access list writes over the previously entered access list.You must enter the **shutdown** and **no shutdown** commands to make the new access list take effect.

Create an ACL list using the **ip access-list** or **ipv6 access-list** command. When you configure an ACL to use with IP multiplexing, filter only traffic based on destination address, destination port, and protocol type. If you configure an ACL with other filter characteristics, unexpected or undesirable multiplexing decisions may occur. If you change an ACL associated with an IP Multiplexing profile, you will be prompted to issue a shutdown/no shutdown to the profile before the new access-list filters take effect.

If you delete an ACL from the profile, IP multiplexing will not send superframes, however it will still accept superframes.

Examples

The following example shows how to configure the ACL *routeRTP-SJ* as the active ACL to filter packets for IP multiplexing.

```
router#configure terminal
router(config)#ipv6 mux profile routeRTP-SJ
router(config-ipmux-v6)#access-list routeRTP-SJ
router(config-ipmux-v6)#exit
router(config)#
```

clear dlep client

To clear a router-to-radio peer association, use the **clear dlep client** command in privileged EXEC mode.

clear dlep client [*interface*] [*peer-id*]

Syntax Description

interface	FastEthernet or VLAN
peer-id	Peer ID with valid range from 1 to 2147483647. Clears a specific router-to-radio peer association (client) identified in the output of the **show dlep clients** command.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)GC	This command was introduced.

Usage Guidelines

Use this command to clear a router-to-radio peer association.

The following example clears a router-to-radio peer association on the fa0/1 interface (with a peer ID value of 11):

```
Router# clear dlep client fa0/1 11
```

Related Commands

Command	Description
show dlep clients	Displays router-to-radio peer associations.

clear dlep counters

To clear DLEP counters, use the **clear dlep counters** command in privileged EXEC mode.

clear dlep counters [*interface*]

Syntax Description

interface	(Optional) Interface where DLEP is configured.

Command Default

If no arguments are specified, all counters on all VMI interfaces with DLEP configured are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Examples

The following example shows how to clear counters on one DLEP interface:

```
Router# clear dlep counters gigabitEthernet 0/1.5
```

clear dlep neighbor

To clear a neighbor session, use the **clear dlep neighbor** command in privileged EXEC mode.

clear dlep neighbor [*interface*] [*session-id*]

Syntax Description

interface	FastEthernet or VLAN
session-id	Session ID with valid range from 1 to 2147483647 Clears a neighbor session with a specific neighbor identified in the output of the **show dlep neighbors** command

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)GC	This command was introduced.

Usage Guidelines

Use this command to clear the neighbor session on the specified interface.

Examples

The following example clears a DLEP neighbor session on a specific FastEthernet interface—where the interface is fa0/1 and the session ID is 11:

```
Router# clear dlep neighbor fa0/1 11
```

Related Commands

Command	Description
show dlep neighbors	Displays neighbor sessions on the specified interface.

clear ospfv3

To clear redistribution by the IPv4 OSPFv3 routing process, use the **clear ospfv3** command in privileged EXEC mode.

clear ospfv3 [*process-id*] {**counters** [**neighbor** [*neighbor-interface*] [*neighbor-id*] **| force-spf | process | redistribution | traffic** [*interface-id*]]}

Syntax Description

process-id	(Optional) Process ID.
counters	OSPF counters.
neighbor	(Optional) Neighbor statistics per interface.
neighbor-interface	(Optional) Neighbor interface.
neighbor-id	(Optional) Neighbor ID.
force-spf	Run SPF for the OSPF process.
process	Reset the OSPF process.
redistribution	Clear OSPF route redistribution.
traffic	Clear traffic-related statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)GC	This command was introduced.

Usage Guidelines

Use the *process-id* argument to clear only one OSPF process. If *process-id* is not specified, all OSPF processes are cleared.

Examples

The following example clears all OSPFv3 processes:

```
router# clear ospfv3 process

Reset ALL OSPFv3 processes? [no]: yes
router#
```

The following example clears the OSPFv3 counters for neighbor s19/0.

```
router# clear ospfv3 counters neighbor s19/0

Reset OSPFv3 counters? [no]: yes
router#
```

The following example now shows that there have been 0 state changes since using the **clear ospfv3 counters neighbor s19/0** command:

```
Router# show ospfv3 counters neighbor detail

Neighbor 172.16.4.4
```

```
    In the area 0 via interface POS4/0
    Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63AD1B0D
    Dead timer due in 00:00:33
    Neighbor is up for 00:48:56
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.3.3
    In the area 1 via interface FastEthernet0/0
    Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 172.16.6.6 BDR is 172.16.3.3
    Options is 0x63F813E9
    Dead timer due in 00:00:33
    Neighbor is up for 00:09:00
    Index 1/1/2, retransmission queue length 0, number of retransmission 2
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.5.5
    In the area 2 via interface ATM3/0
    Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63F7D249
    Dead timer due in 00:00:38
    Neighbor is up for 00:10:01
    Index 1/1/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
Router#
```

The following example shows the **clear ospfv3 force-spf** command:

```
Router1#clear ospfv3 force-spf
```

The following example clears all OSPF processes:

```
router# clear ospfv3 process

Reset ALL OSPFv3 processes? [no]: yes
router#
```

The following example clears all OSPF processes for neighbors:

```
router# clear ospfv3 process neighbor
```

The following example shows the **clear ospfv3 redistribution** command:

```
router# clear ospfv3 redistribution
```

The following example shows the **clear ospfv3 traffic** command:

```
router# clear ospfv3 traffic
```

Related Commands

Command	Description
show ospfv3 neighbor	Displays OSPF neighbor information on a per-interface basis.

clear pppoe relay context

To clear the PPP over Ethernet (PPPoE) relay context created for relaying PPPoE Active Discovery (PAD) messages, use the **clear pppoe relay context** command in privileged EXEC mode.

clear pppoe relay context {**all** | **id** *session-id*}

Syntax Description

all	Clears all relay contexts.
id session-id	Clears a specific context identified in the output of the **show pppoe relay context all** command.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to clear relay contexts created for relaying PAD messages.

Examples

The following example clears all PPPoE relay contexts created for relaying PAD messages:

```
Router# clear pppoe relay context all
```

Related Commands

Command	Description
show pppoe relay context all	Displays PPPoE relay contexts created for relaying PAD messages.
show pppoe session	Displays information about currently active PPPoE sessions.

clear vmi counters

To clear VMI counters, use the **clear vmi counters** command in privileged EXEC mode.

clear vmi counters [*vmi-interface*]

Syntax Description

vmi-interface	(Optional) Number assigned to the VMI.

Command Default

If no VMI interfaces are specified, counters on all VMI interfaces are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Examples

The following example shows how to clear counters on VMI 1:

```
Router# clear vmi counters vmi1
```

destination

To specify the IPv4 or IPv6 destination address for the remote endpoint of the IP multiplexing path, enter the **destination** command. To clear the destination address, use the **no** form of the command.

destination {*ip_addr* | *ipv6_addr*}

[**no**] **destination**

Syntax Description

ip_addr	IPv4 address for the destination remote endpoint of the IP multiplexing path.
ipv6_addr	IPv6 address for the destination remote endpoint of the IP multiplexing path.

Command Modes

IP multiplexing configuration (config-ipmux-profile)

IPv6 multiplexing configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

You must configure a destination address for the profile in order to use it. If you attempt to issue a no shutdown command when no destination address is configured, you will be prompted to configure a destination address. If a profile is active, you must issue a shutdown command before changing the destination address.

An incoming superframe must match its source and destination addresses to the destination and source addresses, respectively, in the multiplexing profile in order for the superframe to be demultiplexed. If either address does not match, the superframe is ignored.

If you enter the **destination** command again, then the new address overwrites the previously entered address.

Examples

The following example shows how to configure the IPv6 address *FE80::A8BB:CCFF:FE01:5700* as the destination address for superframe packets.

```
router#configure terminal
router(config)#ipv6 mux profile routeRTP-SJ
router(config-ipmux-v6)#destination FE80::A8BB:CCFF:FE01:5700
router(config-ipmux-v6)#exit
router(config)#
```

eigrp interface

To set a threshold value to minimize hysteresis in a router-to-radio configuration, use the **eigrp interface** command in interface-configuration mode. To reset the hysteresis threshold to the default value, use the **no** form of this command.

eigrp *vmi-interface-number* **interface** [**dampening-change** *value*] [**dampening-interval** *value*]

no eigrp *vmi-interface-number* **interface** [**dampening-change** *value*] [**dampening-interval** *value*]

Syntax Description

vmi-interface-number	The number assigned to the Virtual Multipoint Interface (VMI).
dampening-change *value*	(Optional) Value used to minimize the effect of frequent routing changes in router-to-radio configurations. Percent interface metric must change to cause update. Value ranges from 1 to 100.
dampening-interval *value*	(Optional) Specifies the time interval in seconds to check the interface metrics at which advertising of routing changes occurs. The default value is 30 seconds. Value ranges from 1 to 65535

Command Default

Default for change-based dampening is 50 percent of the computed metric.

Default for interval-based dampening is 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command advertises routing changes for Enhanced Interior Gateway Routing Protocol (EIGRP) traffic only.

The REPLY sent to any QUERY always contains the latest metric information. Exceptions that result in an immediate UPDATE being sent include the following replies:

- A down interface
- A down route
- Any change in metric which results in the router selecting a new next hop

Change-based Dampening

The **default** value for the change tolerance will be 50 percent of the computed metric. It can be configured in a range of 0 to 100 percent. If the metric change of the interface is not greater (or less) than the current metric plus or minus the specified amount, the change will not result in a routing change, and no update will be sent to other adjacencies.

Interval-based Dampening

The **default** value for the update intervals is 30 seconds. It can be configured in the range from 0 to 64535 seconds. If this option is specified, changes in routes learned though this interface, or in the interface metrics, will not be advertised to adjacencies until the specified interval is met. When the timer expires, any changes detected in any routes learned through the interface, or the metric reported by the interfaces will be sent out.

Examples

Change-based Dampening Example

The following example sets the threshold to 50 percent tolerance routing updates involving VMI interfaces and peers:

```
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 ipv6 address 2001:0DB1:2::1/96
 ipv6 enable
 eigrp 1 interface dampening-change 50
 physical-interface Ethernet0/0
```

Interval-based Dampening Example

The following example sets the interval to 30 seconds at which updates occur for topology changes that affect VMI interfaces and peers:

```
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 ipv6 address 2001:0DB1:2::1/96
 ipv6 enable
 eigrp 1 interface dampening-interval 30
 physical-interface Ethernet0/0
```

Related Commands

Command	Description
debug vmi	Displays debugging output for VMIs.
eigrp interface	Sets a threshold value to minimize hysteresis in a router-to-radio configuration.
interface vmi	Creates a VMI that can be configured and applied dynamically.

flowcontrol send

To enable transmit flow control on an interface, use the **flowcontrol send** command in interface-configuration mode. To disable transmit flow control, use the **no** form of this command.

flowcontrol send

no control send

Command Default

Transmit flow control is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(1)GC	This command was introduced.

Examples

The following example shows how to enable transmit flow control on interface FastEthernet 0/0:

```
router (config)#interface fastethernet0/0
router (config-if)#flowcontrol send
router (config-if)#end
```

holdtime

To specify the amount of time, in milliseconds, that a multiplex profile waits to fill the superframe before sending a partial superframe with currently queued packets, enter the **holdtime** command. To reset the holdtime to 20 milliseconds, use the **no** form of the command.

holdtime {*milliseconds*}

[**no**] **holdtime**

Syntax Description

milliseconds	Amount of time that a multiplex profile waits before sending a partial superframe. Valid values range from 20 to 250 milliseconds.

Command Modes

IP multiplexing configuration (config-ipmux-profile)

IPv6 multiplexing configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

If you do not enter a holdtime, the profile waits the default value of 20 milliseconds before sending a partial superframe.

Examples

The following example shows how to configure the hold time to 150 milliseconds before the profile forwards a partial superframe.

```
router#configure terminal
router(config)#ipv6 mux profile routeRTP-SJ
router(config-ipmux-v6)#holdtime 150
router(config-ipmux-v6)#exit
router(config)#
```

interface vmi

To create a Virtual Multipoint Interface (VMI) for dynamic configuration and application, use the **interface vmi** command in global-configuration mode. To remove a VMI interface, use the **no** form of this command.

interface vmi *interface-number*

no interface vmi *interface-number*

Syntax Description

interface-number	Number assigned to the VMI. The value range for VMI interface numbers is from 1 to 2147483647.

Command Default

No VMI is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

VMI Interface Aggregation Point

The VMI interface acts as an aggregation point for multiple PPPoE connections from one or more radios over one or more physical interfaces.

OSPFv3 and EIGRP Route Advertisements

All OSPFv3, EIGRPv4, and EIGRPv6 route advertisements that are received over the PPPoE connections are reported to the routing protocol as coming from a single interface, thus simplifying the routing protocol topology table and providing scalability benefits of each of the routing protocols.

Examples

The following example shows how to create a VMI interface:

```
interface vmi 1
ip address 10.2.1.1 255.255.255.0
ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64
ipv6 enable
physical-interface GigabitEthernet 0/0
end
```

Related Commands

Command	Description
debug vmi	Displays debugging output for VMIs.
eigrp interface	Sets a threshold value to minimize hysteresis in a router-to-radio configuration.
mode bypass	Enables VMIs to support multicast traffic.
physical interface	Creates a physical subinterface to be associated with the VMIs on a router.

ip dlep set heartbeat-threshold

To set the maximum number of consecutively missed heartbeats allowed on the DLEP router-to-radio association, use the **ip dlep set heartbeat-threshold** command in interface-configuration mode.

ip dlep set heartbeat-threshold *count*

Syntax Description

count	Maximum number of missed heartbeats allowed. The valid range is from 2 to 8.

Command Default

The default DLEP heartbeat threshold is 4.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)GC	This command was introduced.

Usage Guidelines

Use the **ip dlep set heartbeat-threshold** command to set the maximum number of consecutively missed heartbeats allowed on the DLEP router-to-radio association before declaring a failed association.

Examples

The following example sets the DLEP heartbeat threshold to 4:

```
Router(config-if)# ip dlep set heartbeat-threshold 4
```

ip dlep set nbr-activity-timeout

To set the maximum time allowed for inactivity before ending a neighbor session, use the **ip dlep set nbr-activity-timeout** command in interface-configuration mode. To reset the timeout to the default value, use the **no** form of this command.

ip dlep set nbr-activity-timeout *seconds*

no ip dlep set nbr-activity-timeout *seconds*

Syntax Description

seconds	The valid range is from 0 to 240 seconds.

Command Default

The default neighbor-activity timeout is 0 (the timer is disabled).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)GC	This command was introduced.

Usage Guidelines

Use the **ip dlep set nbr-activity-timeout** command to set the maximum number of seconds before a neighbor session-timer determines a neighbor session is stale.

Examples

The following example sets the neighbor-activity timeout to 2 seconds:

```
Router(config-if)# ip dlep set nbr-activity-timeout 2
```

ip dlep set nbr-down-ack-timeout

To set the maximum number of seconds allowed for neighbor sessioning against a lost neighbor-down acknowledgement, use the **ip dlep set nbr-down-ack-timeout** command in interface-configuration mode. To reset the timeout to the default value, use the **no** form of this command.

ip dlep set nbr-down-ack-timeout *seconds*

no ip dlep set nbr-down-ack-timeout *seconds*

Syntax Description

seconds	The valid range is from 0 to 50 seconds.

Command Default

The default neighbor-down-ack timeout is 10 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)GC	This command was introduced.

Usage Guidelines

Use the **ip dlep set nbr-down-ack-timeout** command to set the maximum number of seconds allowed for neighbor sessioning against a lost neighbor-down acknowledgement.

Examples

The following example sets the neighbor-down-ack timeout to 12 seconds:

```
Router(config-if)# ip dlep set nbr-down-ack-timeout 12
```

ip dlep set peer-terminate-ack-timeout

To set the maximum number of seconds allowed for neighbor sessioning against a lost peer-terminate-acknowledgement, use **ip dlep set peer-terminate-ack-timeout** command in interface-configuration mode. To reset the timeout to the default value, use the **no** form of this command.

ip dlep set peer-terminate-ack-timeout *seconds*

no ip dlep set peer-terminate-ack-timeout *seconds*

Syntax Description

seconds	The valid range is from 0 to 50 seconds.

Command Default

The default neighbor-down-ack timeout is 10 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)GC	This command was introduced.

Usage Guidelines

Use the **ip dlep set nbr-down-ack-timeout** command to set the maximum number of seconds allowed for neighbor sessioning against a lost peer-terminate-acknowledgement.

Examples

The following example sets the neighbor-down ack timeout to 12 seconds:

```
Router(config-if)# ip dlep set peer-terminate-ack-timeout 12
```

ip dlep vtemplate

To initiate DLEP on the interface (and set the virtual-template interface number), use the **ip dlep vtemplate** command in interface-configuration mode. To disable DLEP on the interface, use the **no** form of this command.

ip dlep vtemplate *number* [**port** *number*]

no ip dlep vtemplate *number* [**port** *number*]

Syntax Description

vtemplate	Sets the virtual-template interface number for DLEP.
number	The valid range is from 1 to 4096.
port *number*	(Optional) Keyword and port number to designate the port used for the virtual-template interface. The port number valid range is from 1 to 65534.

Command Default

If you do not specify a port number, the default port number used is 55555.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)GC	This command was introduced.

Usage Guidelines

Use the **ip dlep vtemplate** command to specify a virtual-template interface number for DLEP. When assigning this number, you are initiating DLEP on the interface.

To change the virtual-template interface number for DLEP, you must enter the **no** version of the last **ip dlep vtemplate** command you entered before entering the new **ip dlep vtemplate** command.

Examples

The following example shows how to set the DLEP virtual-template interface number to 88:

```
Router(config-if)# ip dlep vtemplate 88
```

The following example shows how to set the DLEP virtual-template interface number to 88 and then change it to 96:

```
Router(config-if)# ip dlep vtemplate 88
Router(config-if)# no ip dlep vtemplate 88
Router(config-if)# ip dlep vtemplate 96
```

ip mux

To enable IP multiplexing on an interface enter the ip mux command. To disable IP multiplexing on an interface use the no form of the command.

{**ip** | **ipv6**} **ip mux**

[**no**] {**ip** | **ipv6**} **ip mux**

SyntaxDescription

{**ip** | **ipv6**} **ip mux**	To enable IP multiplexing on an interface enter the ip mux command.
[**no**] {**ip** | **ipv6**} **ip mux**	To disable IP multiplexing on an interface use the no form of the command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

IP multiplexing must be enabled on the interface for the interface to receive or send IP multiplexing superframes.

Examples

The following example shows how to configure IP multiplexing in IPv6 on interface FastEthernet 0/1.

```
router#configure terminal
router(config)#interface fastethernet0/1
router(config-if)#ipv6 address FE80::A8BB:CCFF:FE01:5700
router(config-if)#ipv6 enable
router(config-if)#ip mux
router(config-if)#exit
router(config)#
```

ip mux cache

To set the IP multiplex cache size in bytes, enter the ip mux cache command.

ip mux cache *size*

Syntax Description

size	Maximum cache size in bytes. Valid values range from 1000000 to 4294967295.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

If you do not enter a cache size, the IP multiplexing packet handler defaults to 1,000,000 bytes. A 1,000,000 byte cache contains 11363 entries.

Examples

The following example shows how to configure the IP multiplexing cache size to 5,000,000.

```
router#configure terminal
router(config)#ip mux cache 5000000
router(config)#
```

ip mux policy

To create an IP multiplexing DSCP policy with a specified name and enter IP multiplexing policy mode, enter the **ip mux policy** command. To delete the IP multiplexing policy, use the **no** form of this command.

{**ip** | **ipv6**} **mux policy** *policy_name*

[**no**] {**ip** | **ipv6**} **mux policy** *policy_name*

Syntax Description

ip	Keyword to specify an IPv4 multiplexing DSCP policy and enter IP multiplexing policy configuration mode.
ipv6	Keyword to specify an IPv6 multiplexing DSCP policy and enter IPv6 multiplexing policy configuration mode.
policy_name	Name of the IP multiplexing policy.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

You can specify up to three policies in addition to the default policy.

Examples

The following example shows how to configure an IPv6 multiplexing DSCP policy with the name *routeRTP-SJ* and enter IPv6 multiplexing policy configuration mode.

```
router#configure terminal
router(config)#ipv6 mux policy routeRTP-SJ
router(config-ipmux-policy-v6)#
```

ip mux profile

To create an IP multiplexing profile with a specified name and enter IP multiplexing profile mode, enter the **ip mux profile** command. To delete the IP multiplexing profile, use the **no** form of this command.

{**ip** | **ipv6**} **mux profile** *profile_name*

[**no**] {**ip** | **ipv6**} **mux profile** *profile_name*

Syntax Description

ip	Keyword to specify an IPv4 multiplexing profile and enter IP multiplexing profile configuration mode.
ipv6	Keyword to specify an IPv6 multiplexing profile and enter IPv6 multiplexing profile configuration mode.
profile_name	Name of the IP multiplexing profile.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

There is no default profile. You can specify up to 500 profiles.

Examples

The following example shows how to configure an IPv6 multiplexing profile with the name *routeRTP-SJ* and enter IPv6 multiplexing profile configuration mode.

```
router#configure terminal
router(config)#ipv6 mux profile routeRTP-SJ
router(config-ipmux-profile-v6)#
```

ip mux udpport

To specify a destination UDP port to use for multiplexed packets, enter the ip mux udpport command.

ip mux udpport *port_number*

Syntax Description

port_number	UDP port number. Valid values range from 1024 to 49151.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

If you do not enter a port number, the system uses the default port 6682.

Examples

The following example shows how to configure the UDP port or IP multiplexing packets to 5000.

```
router#configure terminal
router(config)#ip mux udpport 5000
router(config)#
```

ip r2cp heartbeat-threshold

To set the maximum number of missed R2CP heartbeat messages allowed before declaring the router-to-radio association failed, use the **ip r2cp heartbeat-threshold** command in interface-configuration mode.

ip r2cp heartbeat-threshold *count*

Syntax Description

heartbeat-threshold	The number of missed R2CP heartbeats allowed before declaring a failed association between the router and locally attached radio.
count	The valid range is from 2 to 8.

Command Default

The default R2CP heartbeat threshold is 3.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

Use the **ip r2cp heartbeat-threshold** command to set the R2CP heartbeat threshold. This heartbeat threshold is the number of consecutively missed R2CP heartbeats allowed before declaring the router-to-radio association failed.

Examples

The following example sets the R2CP heartbeat threshold to 3:

```
Router(config-if)# ip r2cp heartbeat-threshold 3
```

ip r2cp node-terminate-ack-threshold

To set the R2CP node-terminate acknowledgement threshold, use the **ip r2cp node-terminate-ack-threshold** command in interface-configuration mode. To reset the default-node terminate acknowledgement threshold to the default value, use the **no** form of this command.

ip r2cp node-terminate-ack-threshold *value*

no ip r2cp node-terminate-ack-threshold *value*

Syntax Description

node-terminate-ack-threshold	The number of missed and/or lost R2CP node acknowledgements allowed before declaring the terminate effort complete.
value	The valid range is from 1 to 5.

Command Default

The default R2CP node-terminate acknowledgement threshold is 3.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

Use the **ip r2cp node-terminate-ack-threshold** command to set the number of missed and/or lost R2CP node acknowledgements allowed before declaring the terminate effort complete.

Examples

The following example sets the R2CP node-terminate-ack-threshold to 2:

```
Router(config-if)# ip r2cp node-terminate-ack-threshold 2
```

Related Commands

Command	Description
node-terminate-ack-timeout	Sets the number of milliseconds the client waits for the node-terminate acknowledgment.

ip r2cp node-terminate-ack-timeout

To set the R2CP node-terminate acknowledgement timeout, use the **ip r2cp node-terminate-ack-timeout** command in interface-configuration mode. To reset the R2CP node-terminate acknowledgement timeout to the default value, use the **no** form of this command.

ip r2cp node-terminate-ack-timeout *milliseconds*

no ip r2cp node-terminate-ack-timeout *milliseconds*

Syntax Description

node-terminate-ack-timeout	The maximum number of milliseconds allowed by R2CP when waiting for the node-terminate acknowledgement.
milliseconds	The timeout range is between 100 and 5000 milliseconds.

Command Default

The default node-terminate acknowledgement timeout is 1000 milliseconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

Use the **ip r2cp node-terminate ack-timeout** command to set the maximum number of milliseconds the client can wait for a node-terminate acknowledgement.

Examples

The following example sets the node-terminate acknowledgement timeout to 2200 milliseconds for R2CP:

```
Router(config-if)# ip r2cp node-terminate-ack-timeout 2200
```

Related Commands

Command	Description
node-terminate-ack-threshold	Sets the number of missed and/or lost node acknowledgements allowed by R2CP before declaring the terminate effort complete.

ip r2cp port

To specify a port for R2CP , use the **ip r2cp port** command in interface-configuration mode. To reset the R2CP port number to the default value, use the **no** form of this command.

ip r2cp port *number*

no ip r2cp port *number*

Syntax Description

port	The port specified for R2CP.
number	The port number valid range is from 1 to 65534.

Command Default

The default port number is 28672.

Command Modes

Interface configuration (config-if)

Command History

Release	**Modification**
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

Use the **ip r2cp port** command to specify the port for R2CP.

Examples

The following example sets the R2CP port to 5858:

```
Router(config-if)# ip r2cp port 5858
```

ip r2cp session-activity-timeout

To configure the R2CP neighbor session-activity timeout, use the **ip r2cp session-activity-timeout** command in interface-configuration mode. To reset the neighbor session-terminate activity timeout to the default value, use the **no** form of this command.

ip r2cp session-activity-timeout *seconds*

no ip r2cp session-activity-timeout *seconds*

Syntax Description

session-activity-timeout	The port specified for R2CP.
seconds	The valid range for R2CP neighbor session-activity timeout is from 0 to 4 seconds.

Command Default

The default neighbor session-activity timeout is 1 second.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

Use the **ip r2cp session-activity-timeout** command to set the maximum number of seconds before a neighbor session-timer determines a neighbor session is stale.

Examples

The following example sets the neighbor-session activity timeout for R2CP to 2 seconds:

```
Router(config-if)# ip r2cp session-activity-timeout 2
```

ip r2cp session-terminate-ack-threshold

To set the R2CP neighbor session-terminate acknowledgement threshold, use the **ip r2cp session-terminate-ack-threshold** command in interface-configuration mode. To reset the R2CP neighbor session terminate-acknowledgement threshold to the default value, use the **no** form of this command.

ip r2cp session-terminate-ack-threshold *value*

no ip r2cp session-terminate-ack-threshold *value*

Syntax Description

session-terminate-ack-threshold	The number of missed and/or lost R2CP neighbor session acknowledgements allowed before declaring the terminate effort complete.
value	The value range is from 1 to 5 sessions.

Command Default

The default neighbor session-terminate acknowledgement threshold is 3.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

Use the **ip r2cp session-terminate-acknowledgement-threshold** command to set the number of missed and/or lost R2CP neighbor session acknowledgements allowed before declaring the terminate effort complete.

Examples

The following example sets the R2CP neighbor session-terminate acknowledgement threshold to 4:

```
Router(config-if)# ip r2cp session-terminate-ack-threshold 4
```

Related Commands

Command	Description
session-terminate-ack-timeout	Sets the amount of time the client waits for the neighbor session terminate acknowledgment in milliseconds.

ip r2cp session-terminate-ack-timeout

To set the maximum number of milliseconds allowed on the R2CP interface before sending a neighbor session terminate-acknowledgement, use the **ip r2cp session-terminate-ack-timeout** command in interface-configuration mode. To reset the timeout to the default value, use the **no** form of this command.

ip r2cp node-terminate-ack-timeout *milliseconds*

no ip r2cp node-terminate-ack-timeout *milliseconds*

Syntax Description

session-terminate-ack-timeout	The time duration allowed by R2CP when waiting for the neighbor session-terminate acknowledgement.
milliseconds	The timeout range is between 100 and 5000 milliseconds.

Command Default

The neighbor session terminate-acknowledgement timeout default is 1000 milliseconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

Use the **ip r2cp session-terminate-ack-timeout** command to set the amount of time the client waits for the node terminate acknowledgement to occur in milliseconds.

Examples

The following example sets the neighbor session terminate-acknowledgement timeout to 2400 milliseconds for R2CP:

```
Router(config-if)# ip r2cp session-terminate-ack-timeout 2400
```

Related Commands

Command	Description
session-terminate-ack-threshold	Sets the number of missed and/or lost session acknowledgements allowed by R2CP before declaring the terminate effort complete.

ip r2cp virtual-template

To set a virtual-template access number for R2CP, use the **ip r2cp virtual-template** command in interface-configuration mode. To free a virtual template from R2CP, use the **no** form of this command.

ip r2cp virtual-template *number*

no ip r2cp virtual-template *number*

Syntax Description

virtual-template	Sets the virtual-template access number for R2CP.
number	The valid range is from 0 to 21474883647.

Command Default

The default virtual-template number is 0.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

Use the **ip r2cp virtual-template** command to specify a virtual-template access number for R2CP. When creating a virtual-access interface, R2CP requires this access number for virtual-template selection.

Examples

The following example sets the R2CP virtual-template access number to 224:

```
Router(config-if)# ip r2cp virtual-template 224
```

manet cache

To configure the number of MANET cached LSA updates and acknowledgments, use the **manet cache** command in router-configuration mode. To restore the default values, use the **no** form of this command.

manet cache {**update** *update-value* | **acknowledgment** *ack-value*}

no manet cache {**update** | **acknowledgment**}

Syntax Description

update	Cached LSA updates.
update-value	The number of cached LSA updates. The value ranges from 0 to 4294967295. The default value is 1000.
acknowledgment	Cached LSA acknowledgments.
ack-value	The number of cached LSA acknowledgments. The value ranges from 0 to 4294967295. The default value is 1000.

Defaults

1000 updates or 1000 acknowledgments

Command Modes

Router configuration (config-router)

CommandHistory

Release	Modification
12.4(24) GC	This command was introduced.

Setting the Cache Size

When you set the cache size, the router keeps a larger number of temp LSAs and ACKs. If the cache fills up before the timers expire, the LSAs and ACKs are deleted from the cache. In some cases, the deleted ACKs can cause the router to flood 1-hop neighbors because the router no longer knows about the deleted ACKs.

Increasing the Cache Size

If you increase the size of the cache, you might prevent non-primary relay routes from flooding in the case when ACKs were deleted because the cache became full before the ACK timer expired. Increasing the cache size reduces the amount of memory available for the cache storage.

Caution Before you decide to increase the cache size, ensure that the free memory is not reduced to levels that can affect basic route processing.

Assessing How Cache Size Affects Performance

It is difficult to assess the number of times that flooding occurs because LSAs and ACKs have been deleted before the ACK timer expired. Use the **show ospfv3** command to compare the current and maximum cache values. Over time, if the two values are very close, it indicates that the cache is filling up faster than the timer expiration is occurring. In that case, increasing the cache size may be helpful.

Examples

The following example uses cache size for the LSA update and LSA ACKs. The **manet cache update** command optimizes the exchange of the LS database while forming adjacencies with new neighbors in the radio environment. The result is minimized OSPF control traffic and reduced use of radio bandwidth. The ACK cache size improves the dynamic relaying of the LSA update information:

```
Router(config)# ipv6 unicast-routing
Router(config)# router ospfv3 1
Router(config-router)# manet cache acknowledgment 2000
Router(config-router)# manet cache update 2000
Router(config-router)# ^Z

Router# show ospfv3 1
Routing Process "ospfv3 1" with ID 172.27.76.13
 Supports IPv6 Address Family
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Initial SPF schedule delay 1000 msecs
 Minimum hold time between two consecutive SPFs 2000 msecs
 Maximum wait time between two consecutive SPFs 2000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 Relay willingness value is 128
 Pushback timer value is 2000 msecs
 Relay acknowledgement timer value is 1000 msecs
 LSA cache Enabled : current count 0, maximum 2000
 ACK cache Enabled : current count 0, maximum 2000
 Selective Peering is not enabled
 Hello requests and responses will be sent multicast
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 1
        SPF algorithm executed 2 times
        Number of LSA 2. Checksum Sum 0x0116AD
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

The lines that begin with "LSA cache Disabled" and "ACK cache Disabled" contain the cache size information.

Related Commands

Command	Description
timers manet	Configures MANET timer parameters.

manet hello unicast

To configure whether MANET hello requests and responses are sent as unicast packets or multicast packets use the **manet hello unicast** command in router-configuration mode. To return to multicast MANET hello requests, use the **no** form of this command.

manet hello unicast

no manet hello unicast

Syntax Description

unicast	Configures manet hello requests and responses to send in unicast.

Command Default

The default is multicast manet hello requests.

Command Modes

Router configuration (config-rtr)

Command History

Release	Modification
12.4(24) GC	This command was introduced.

Usage Guidelines

For broadcast radios, multicast mode typically provides improved performance with reduced bandwidth utilization. For point-to-point radios, unicast mode typically provides improved performance and reduced bandwidth utilization.

Note For optimal performance, configure all nodes consistently.

Examples

The following example shows how to configure the **manet hello unicast** command.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# router ospfv3 1
Router(config-rtr)# manet hello unicast
Router(config-rtr)# end
```

manet peering selective

To enable selective peering on a per-area or per-interface basis and configure the maximum number of redundant paths to each neighbor, use the **manet peering selective** command in router-configuration mode. To disable selective MANET peering, use the **no** form of this command.

manet peering selective [**redundancy** *redundancy-count*] [**per-interface**]

no manet peering selective

Syntax Description

redundancy	To only count redundant paths on a per-interface basis, rather than across all interfaces.
redundancy-count	Change the preferred number of redundant paths to any given peer. The default redundancy count if not specified is 1 (2 paths).
per-interface	To only specify the maximum number of redundant paths desired to a given peer. The range of this value is 0-10. A value of 0 indicates only a single path is desired.

Command Modes

Router configuration (config-rtr)

Command History

Release	Modification
12.4(24) GC	This command was introduced.

Usage Guidelines

Selective peering will only be enabled for instances of the OSPF process for which the corresponding interface have been configured with the **ospfv3 network manet** command.

Examples

The following example shows how to enable manet selective peering per interface with a redundancy of 10.

```
router(config)#router ospfv3 1
router(config-rtr)#manet peering selective per-interface redundancy 10
```

manet willingness

To configure the overlapping relay willingness value on a MANET router, use the **manet willingness** command in router-configuration mode. To disable a willingness value, use the **no** form of this command which restores the default willingness value of 128.

manet willingness *will-value*

no manet willingness

Syntax Description

will-value	The willingness value range is from 0 to 255.

Defaults

The willingness default value is 128.

Command Modes

Router configuration (config-rtr)

Command History

Release	Modification
12.4(24) GC	This command was introduced.

Usage Guidelines

Willingness is a one-octet unsigned integer describing the willingness of the sender to act as an active overlapping relay for its peers. A willingness value of 100 is less willing to become a relay than a value of 128.

A willingness value of 0 means that the router will NEVER be chosen as an active relay by its peers. A willingness value of 255 means that the router will ALWAYS be chosen as an active relay by its peers.

Examples

The following example shows how to controls the willingness of the router to be an active relay for the MANET network:

```
Router(config)# router ospfv3 100
Router(config-rtr)# manet willingness 100
Router(config-rtr)# end
Router# show ospfv3 100
Routing Process "ospfv3 100" with ID 5.5.5.5
 Supports IPv6 Address Family
 Supports Link-local Signaling (LLS)
 It is an autonomous system boundary router
 Redistributing External Routes from,
 connected
 SPF schedule delay 1 secs, Hold time between two SPFs 1 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 3. Checksum Sum 0x00AAB6
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Reference bandwidth unit is 100 mbps
```

```
Relay willingness value is 100
Pushback timer value is 2000 msecs
Relay acknowledgement timer value is 1000 msecs
LSA cache Enabled : current count 0, maximum 1000
ACK cache Enabled : current count 0, maximum 1000
Selective Peering is not enabled
Hello requests and responses will be sent multicast
Area BACKBONE(0)
Number of interfaces in this area is 1
SPF algorithm executed 2 times
Number of LSA 6. Checksum Sum 0x02D90A
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

Related Commands

Command	Description
show ospfv3	Displays general information about OSPF routing processes.

matchdscp

To specify a DSCP value used to match IP multiplexed packets for the policy, enter the matchdscp command.

matchdscp *DSCP_value*

Syntax Description

DSCP_value	DSCP value. Valid values range from 0 to 63. The following DSCP values are also valid: af11 Match packets with AF11 dscp (001010) af12 Match packets with AF12 dscp (001100) af13 Match packets with AF13 dscp (001110) af21 Match packets with AF21 dscp (010010) af22 Match packets with AF22 dscp (010100) af23 Match packets with AF23 dscp (010110) af31 Match packets with AF31 dscp (011010) af32 Match packets with AF32 dscp (011100) af33 Match packets with AF33 dscp (011110) af41 Match packets with AF41 dscp (100010) af42 Match packets with AF42 dscp (100100) af43 Match packets with AF43 dscp (100110) cs1 Match packets with CS1(precedence 1) dscp (001000) cs2 Match packets with CS2(precedence 2) dscp (010000) cs3 Match packets with CS3(precedence 3) dscp (011000) cs4 Match packets with CS4(precedence 4) dscp (100000) cs5 Match packets with CS5(precedence 5) dscp (101000) cs6 Match packets with CS6(precedence 6) dscp (110000) cs7 Match packets with CS7(precedence 7) dscp (111000) default Match packets with default dscp (000000) ef Match packets with EF dscp (101110)

Command Modes

IP multiplexing policy configuration (config-ipmux-policy)

IPv6 multiplexing policy configuration (config-ipmux-policy-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

Make sure that the DSCP values do not overlap between policies. If the DSCP values do overlap, then the first policy to match the DSCP value from the top of the list is selected.

Examples

The following example shows how to configure the DSCP value to *45* in the IPv6 Multiplexing policy *routeRTP-SJ*.

```
router#configure terminal
router(config)#ipv6 mux policy routeRTP-SJ
router(config-ipmux-policy-v6)#matchdscp 45
router(config-ipmux-policy-v6)#exit
router(config)#
```

maxlength

To specify the largest packet size that the multiplex profile can hold for multiplexing, enter the **maxlength** command. To reset the policy to multiplex any packet that fits in the superframe, use the **no** form of the command.

maxlength *bytes*

[**no**] **maxlength**

Syntax Description

bytes	Maximum packet size in bytes. Valid values range from 64 to 1472 bytes

Command Default

By default, the policy multiplexes any packet that fits into the superframe.

Command Modes

IP multiplexing configuration (config-ipmux-profile)

IPv6 multiplexing configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

If you do not specify a maximum packet size for multiplexing, the maximum packet size will default to the configured MTU size minus the length of the superframe header (28 bytes for IPv4, 48 bytes for IPv6).

Examples

The following example shows how to configure the maximum packet size that can go into the IP multiplexing profile *routeRTP-SJ* to *1472* bytes.

```
router#configure terminal
router(config)#ipv6 mux profile routeRTP-SJ
router(config-ipmux-v6)#maxlength 1472
router(config-ipmux-v6)#exit
router(config)#
```

mode

To enable VMI to support multicast traffic, use the **mode** command in interface-configuration mode. To return the interface to the default mode (aggregate), use the **no** form of this command.

mode {aggregate | bypass}

no mode {aggregate | bypass}

Syntax Description

aggregate	Keyword to set the mode to aggregate. All virtual-access interfaces created by PPPoE neighbor sessions are logically aggregated under the VMI.
bypass	Keyword to set the mode to bypass.

Command Default

The default mode is aggregate.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support multicast traffic on Virtual Multipoint Interfaces (VMIs).

Usage Guidelines

Use this command to support multicast traffic in router-to-radio configurations.

Aggregate Mode

Aggregate mode is the default mode for VMI, where VMI aggregates all virtual-access interfaces logically. To enable VMI to forward packets to the correct virtual-access interface, you must define applications such as EIGRP and OSPFv3 (all applications above Layer 2) on VMI.

Bypass Mode

Using bypass mode is recommended for multicast applications.

In bypass mode, the virtual-access interfaces are directly exposed to applications running above Layer2. In bypass mode, definition of a VMI is still required because the VMI continues to manage presentation of cross-layer signals such as neighbor up, neighbor down, and metrics. However, applications will still be aware on the actual underlying virtual-access interfaces and send packets to them directly.

Using bypass mode can cause databases in the applications to be larger because knowledge of more interfaces are required for normal operation.

After you enter the **mode** command, Cisco recommends that you copy the running configuration to NVRAM because the default mode of operation for VMI is to logically aggregate the virtual-access interfaces.

Examples

The following examples set the interface mode to bypass:

```
Router# enable
Router# configure terminal
Router(config)# interface vmi1
Router(config-if)# mode bypass
```

The following example shows how to enable Multicast Support on a VMI Interface:

Note Enabling Multicast on VMI interfaces includes changing the VMI interface to bypass mode and enabling "ip pim" on the virtual-template interface.

```
!
interface Virtual-Template1
 ip address 4.3.3.1 255.255.255.0
 load-interval 30
 no keepalive
 ip pim sparse-dense-mode
 service-policy output FQ
!
!
interface vmi1
 ip address 4.3.9.1 255.255.255.0
 load-interval 30
 physical-interface FastEthernet0/0
 mode bypass
!
end
```

Related Commands

Command	Description
interface vmi	Creates a VMI interface.

mtu

To specify the maximum transmission unit (MTU) size for an outbound superframe, enter the **mtu** command. To reset the MTU to 1500 bytes, use the **no** form of the command.

mtu *bytes*

[**no**] **mtu**

Syntax Description

bytes	MTU size of the outbound superframe in bytes. Valid values range from 256 to 1500 bytes

Command Default

The maximum superframe packet size is 1500 bytes.

Command Modes

IP multiplexing configuration (config-ipmux-profile)

IPv6 multiplexing configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

If you do not specify an MTU size, the IP multiplex packet handler uses the default value of 1500 bytes.

For each new packet being added to the superframe, the IP multiplex packet handler checks the byte count of the multiplex queue. If the queue byte count and the superframe header length exceeds the configured MTU size, it builds a superframe from the previous packets and the new packet becomes the first packet of the next superframe.

If you enter the **mtu** command again, then the MTU size overwrites the previously entered size.

The superframe size specified in the **mtu** command includes the IP frame header for the superframe of 48 bytes for IPv4 and 28 bytes for IPv4 packets. Therefore an IPv6 mtu configured to 1400 bytes will accept 1352 bytes of data before sending a full superframe. An IPv4 mtu configured to 1400 bytes will accept 1372 bytes of data before sending a full superframe.

Examples

The following example shows how to configure the MTU size for IP multiplexing profile *routeRTP-SJ* to *1000* bytes.

```
router#configure terminal
router(config)#ipv6 mux profile routeRTP-SJ
router(config-ipmux-v6)#mtu 1000
router(config-ipmux-v6)#exit
router(config)#
```

ospfv3 area

To attach an interface to a specific OSPFv3 area and enable routing of IPv6 network traffic using IPv4 or IPv6 addresses, use the **ospfv3 area** command in interface-configuration mode. To detach the interface from the OSPFv3 area, use the **no** form of this command.

ospfv3 *process-id* **area** *area-number* **{ipv4 | ipv6} [instance** *instance-number]*

no ospfv3 [*process-id*] **area** *area-number* **{ipv4 | ipv6} instance** *instance-number*

Syntax Description

process-id	OSPFv3 process ID. This ID number must match the process ID used in the router OSPFv3 global configuration command. The *process-id* is not optional in the **ospfv3 area** command.
area *area-number*	Keyword and area number to specify OSPF area for the OSPF process-id.
ipv4	Keyword to define that the OSPFv3 instance that will use IPv4 routing tables to route IPv6 traffic.
ipv6	Keyword to define that the OSPFv3 instance that will use IPv6 routing tables to route IPv6 traffic.
instance *instance-number*	(Optional) Keyword to specify an OSPFv3 instance with instance number. The valid instance number can range from 0 to 31 of IPv6 address families and 64 to 95 for IPv4 address families. The default IPv6 instance is 0. The default instance for IPv4 is 64.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)GC	This command was introduced.

Usage Guidelines

You must enter this command to attach an interface to a specific OSPFv3 process and instance. After you have attached an interface to a specific OSPFv3 process and interface, you can enter other OSPFv3 characteristics.

An interface can only support one IPv4 address family process and one IPv6 address family process at the same time.

Examples

The following example shows a typical configuration with both IPv6 and IPv4 routing in OSPF that use the default instance numbers.

```
Router(config)# interface ethernet0/0
Router(config-if)# ip address 1.1.1.1 255.0.0.0
Router(config-if)# ospfv3 1 area 0 ipv6
Router(config-if)# ospfv3 2 area 0 ipv4
Router(config-if)#
```

ospfv3 cost dynamic

To specify that the OSPF cost associated with a path on an interface is dynamic, use the **ospfv3 cost dynamic** command in interface-configuration mode.

ospfv3 [*process-id*] **cost dynamic**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.

z

Command Default

By default, MANET interfaces are set to use dynamic costs. Non-MANET networks are set to use static costs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)GC	This command was introduced.

Usage Guidelines

To reset the OSPF cost associated with an interface to a static cost, enter the **OSPFv3 cost** command.

When the network type is set to MANET, the OSPF cost associated with an interface automatically sets to dynamic. All other network types, keep the interface cost, and you must enter the **ospfv3 cost dynamic** command to change the cost to dynamic.

Examples

The following example shows how to configure the OSPFv3 instance 4 to use dynamic costing for the OSPF interface:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface Ethernet 0/0
Router(config-if)# ospfv3 4 cost dynamic
Router(config-if)# exit
```

Related Commands

Command	Description
ospfv3 cost dynamic default	Configure default metric value to use until metric information is received from the radio.
ospfv3 cost hysteresis	Dampen cost changes.
ospfv3 cost dynamic weight	Amount of impact a link metric change has on the dynamic cost.

Command	Description
show ospfv3 interface	Displays information on the OSPFv3 interfaces.
show ospfv3 neighbor manet	Displays information on costs for MANET networks.

ospfv3 cost dynamic default

To specify that the OSPF interface cost associated as dynamic, but use a static value until link metric data arrive, use the **ospfv3 cost dynamic default** command in interface-configuration mode. To reset the interface cost, use the **no** form of this command.

ospfv3 [*process-id*] **cost dynamic default** *interface-cost*

no ospfv3 [*process-id*] **cost dynamic default**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
interface-cost	OSPF interface cost to use until mink metric data arrive. Valid values range from 0 to 65535.

z

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)GC	This command was introduced.

Usage Guidelines

For a MANET interface, if you do not specify a default dynamic cost, OSPF uses the interface cost until it receives link metric data.

Examples

The following example shows how to configure the OSPFv3 instance 4 to use 30 as the default cost until link metric data arrive for dynamic costing:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface Ethernet 0/0
Router(config-if)# ospfv3 4 cost dynamic default 30
Router(config-if)# exit
```

Related Commands

Command	Description
ospfv3 cost hysteresis	Dampen cost changes.
ospfv3 cost dynamic weight	Amount of impact a link metric change has on the dynamic cost.
show ospfv3 interface	Displays information on the OSPFv3 interfaces.
show ospfv3 neighbor manet	Displays information on costs for MANET networks.

ospfv3 cost dynamic hysteresis

To enable cost dynamic hysteresis, use the **ospfv3 cost dynamic hysteresis** command in interface-configuration mode. To disable cost dynamic hysteresis use the **no** form of this command.

ospfv3 [*process-id*] **cost dynamic hysteresis** [**threshold** *threshold_value* | **percent** *percent_value*]

no ospfv3 [*process-id*] **cost dynamic hysteresis** [**threshold** *threshold_value* | **percent** *percent_value*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 0 to 65535.
percent *percent-value*	(Optional) Configure threshold by percentage.The *percent-value* can range from 0 to 100.
threshold *threshold-value*	(Optional) Cost change threshold at which hysteresis will be implemented. The threshold range is from 0 to 64K, and the default threshold value is 10K.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)GC	The **percent** *percent-value* option was added in this version.
12.4(15)T	This command was introduced.

Usage Guidelines

Use this command to dampen the frequency of OSPFv3 route cost changes due to small changes in link metrics. The threshold option specifies the magnitude of change in cost before OSPFv3 is notified. The percent option specifies the change relative to the original cost necessary before OSPFv3 is notified.

The **no ospfv3 cost dynamic hysteresis** command disables cost dynamic hysteresis. The **no ospfv3 cost dynamic hysteresis** command with the **threshold** or **percent** keywords leaves hysteresis enabled and returns the type and value to their defaults.

If hysteresis is enabled without a mode, the default mode is threshold and the default threshold-value is 10.

The higher the threshold or percent value is set, the larger the change in link quality required to change OSPF route costs.

Examples

The following example sets the cost dynamic hysteresis to 10 percent for OSPFv3 process 4:

```
Router(config)# interface vmi1
Router(config-if)# ospfv3 4 cost dynamic hysteresis percent 10
Router(config-if)# end
```

Related Commands

Command	Description
ospfv3 cost dynamic default	Configure default metric value to use until metric information is received from the radio.
ospfv3 cost dynamic weight	Amount of impact a link metric change has on the dynamic cost.
show ospfv3 interface	Displays information on the OSPFv3 interfaces.
show ospfv3 neighbor manet	Displays information on costs for MANET networks.

ospfv3 cost dynamic weight

When dynamic cost is configured, OSPF route cost is calculated from a set of link metrics. To change how each link metric affects route cost, use the **ospfv3 cost dynamic weight** command in interface-configuration mode. The **no** version of this command sets the weight to the default weight for the specified metric.

ospfv3 *process-id* **cost dynamic weight** [**threshold** *threshold_value* | **percent** *percent_value*]

no ospfv3 *process-id* **cost dynamic weight** [**threshold** *threshold_value* | **percent** *percent_value*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
throughput *percent*	Throughput weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
resources *percent*	Resources weight (such as battery life) of the router at the Layer 2 link, expressed as a percentage. The *percent* value can range from 0 to 100. The default value is 100.
latency *percent*	Latency weight of the Layer 2 link, expressed as a percentage. The *percent* value can range from 0 to 100. The default value is 100.
L2-factor *percent*	Quality weight of the Layer 2 link expressed as a percentage. The *percent* value can range from 0 to 100. The default value is 100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)GC	This command was introduced.

Usage Guidelines

The default weight for throughput, resources, latency, and L 2-factor is 100%.

The higher the threshold or percent value is set, the larger the change in link quality required to change OSPF route costs.

Examples

The following example sets the cost dynamic weight for latency to 20%:

```
Router(config)#interface vmi1
Router(config-if)#ospfv3 4 cost dynamic weight latency 20
Router(config-if)#end
```

Related Commands

Command	Description
ospfv3 cost dynamic default	Configure default metric value to use until metric information is received from the radio.
ospfv3 cost hysteresis	Dampen cost changes.
show ospfv3 interface	Displays information on the OSPFv3 interfaces including weights.
show ospfv3 neighbor manet	Displays information on costs for MANET networks.

ospfv3 dead-interval

To set the time period for which hello packets must not be seen before neighbors declare the router down, use the **ospfv3 dead-interval** command in interface-configuration mode. To return to the default time, use the **no** form of this command.

ospfv3 [*process-id*] **dead-interval** *seconds*

no ospfv3 [*process-id*] **dead-interval**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
seconds	Specifies the interval (in seconds). The value must be the same for all nodes on the network.

Command Default

The default interval is four times the interval set by the **ospfv3 hello-interval** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24) GC	This command was introduced.

Usage Guidelines

If no hello-interval is specified, the default dead-interval is 120 second for MANETs and 40 seconds for all other network types.

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 for OSPFv3 process 6:

```
Router(config)#interface etherinet1/0
Router(config-if)#ospfv3 6 dead-interval 60
Router(config-if)#end
Router#
```

Related Commands

Command	Description
ospfv3 hello-interval	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.
ospfv3 network	Specifies the network type for the interface
show ospfv3 interface	Displays information about the OSPFv3 parameters for an interface, including the dead-interval.

ospfv3 hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the interface where the OSPFv3 address family is defined, use the **ospfv3 hello-interval** command in interface-configuration mode. To return to the default time, use the **no** form of this command.

ospfv3 [*process-id*] **hello-interval** *seconds*

no ospfv3 [*process-id*] **hello-interval**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
seconds	Specifies the interval (in seconds). The value must be the same for all nodes on a specific network. The range is from 1 to 65535.

Defaults

30 seconds for MANETs

10 seconds for all other network types

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.(24)GC	This command was introduced.

Usage Guidelines

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

Examples

The following example sets the interval between hello packets to 15 seconds for OSPFv3 process 4:

```
Router(config)#interface Ethernet0/0
Router(config-if)#ospfv3 4 hello-interval 15
Router(config-if)#end
Router#
```

Related Commands

Command	Description
ospfv3 dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router down.
show ospfv3 interface	Displays information about the OSPFv3 parameters for an interface, including the hello-interval.

ospfv3 manet peering cost

Use selective peering to minimize the full neighbor adjacencies in a MANET. To set a minimum cost change threshold necessary before a new neighbor is considered for selective peering, use the **ospfv3 manet peering cost** command in interface-configuration mode. To exclude cost considerations from the selective peering decision, use the **no** form of this command.

ospfv3 [*process-id*] **manet peering cost** {**threshold** *threshold_value* | **percent** *percent_value*}

no ospfv3 [*process-id*] **manet peering cost**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
threshold *threshold-value*	Absolute improvement in cost relative (relative to current cost) necessary to consider a new neighbor for selective peering. Valid values range from 0 to 65535.
percent *percent-value*	Configure threshold by percentage.The *percent-value* can range from 0 to 100.

Command Default

The default MANET peering cost is 0. No incremental improvement in route cost is required to consider selective peering with a new neighbor.

Command Modes

Interface configuration (config-if)

CommandHistory

Release	Modification
12.4(24)GC	This command was introduced.

Usage Guidelines

When selective peering is configured at a given redundancy level, the first 50% of redundant paths do not consider the cost change threshold associated with this command. This allows a minimum OSPFv3 topology to be established in high cost networks.

For example, if you configure selective peering to have a redundancy level of 3 (a total of four paths allowed), the first two neighbors are considered for selective peering, regardless of the neighbor cost. Only the subsequent paths are held to the relative cost change requirements.

Examples

The following example shows how to set the MANET peering cost threshold to 3000.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Ethernet 0/0
Router(config-if)#ospfv3 4 manet peering cost threshold 3000
Router(config-if)#exit
Router(config)#
```

Related Commands

Command	Description
ospfv3 manet peering link-metrics	OSPF may be configured to not respond until metrics and link cost are known.
manet peering selective	Used to enable selective peering on a per-area or per-interface basis and configure the maximum number of redundant paths to each neighbor.

ospfv3 manet peering link-metrics

To configure and OSPFv3 process to wait for link metrics from a neighbor before attempting selective peering with that neighbor, use the **ospfv3 manet peering link-metrics** command in interface-configuration mode. The threshold value specifies a minimum incremental improvement over the existing OSPFv3 route cost before attempting selective peering. The **no** version of the command disables the requirement to wait for link metrics before attempting selective peering.

ospfv3 [*process-id*] **manet peering link-metrics** *threshold*

no ospfv3 [*process-id*] **manet peering link-metrics**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
threshold-value	Absolute improvement in OSPFv3 route cost derived from link metrics necessary to begin selective peering process with neighbor. Valid values range from 0 to 65535.

Command Modes

Interface configuration (config-if)

CommandHistory

Release	Modification
12.4(24)GC	This command was introduced.

Usage Guidelines

By default, selective peering does not require initial link metrics. If you enter this command without a specified threshold, the default threshold is 0.

Examples

The following example shows how to set the peering link metrics threshold to 3000 for OSPFv3 process 4.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Ethernet 0/0
Router(config-if)#ospfv3 4 manet peering link-metrics 3000
Router(config-if)#exit
Router(config)#
```

Related Commands

Command	Description
ospfv3 manet peering cost	Set peering cost for OSPFv3 process.
manet peering selective	Enable selective peering on a per-area or per-interface basis and configure the maximum number of redundant paths to each neighbor.

ospfv3 network

To configure the OSPFv3 network type to a type other than the default for a given medium, use the **ospfv3 network** command in interface-configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **network** {**broadcast** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point** | **manet**}

no ospfv3 [*process-id*] **network**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
network broadcast	Sets the network type to broadcast.
network manet	Sets the network type to MANET.
network non-broadcast	Sets the network type to Non Broadcast Multi Access (NBMA).
network point-to-multipoint [**non-broadcast**]	Sets the network type to point-to-multipoint. The optional **non-broadcast** keyword sets the point-to-multipoint network to non-broadcast. If you use the **non-broadcast** keyword, the **neighbor** command is required.
network point-to-point	Sets the network type to point-to-point.

Defaults

The default network type is broadcast.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)GC	This command was introduced.

Usage Guidelines

MANET Networks

Use the **ospfv3 network manet** command to enable relaying and caching of LSA updates and LSA ACKs on the MANET interface. This will result in a reduction of OSPF traffic and save radio bandwidth

By default, selective peering is disabled on MANET interfaces.

By default, the OSPFv3 dynamic cost timer is enabled for the MANET network type, as well as caching of LSAs and LSA ACKs received on the MANET interface. The following default values are applied for cache and timers:

LSA cache	Default = 1000 messages
LSA timer	Default = 10 minutes

LSA ACK cache	Default = 1000 messages
LSA ACK timer	Default = 5 minutes

NBMA Networks

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 non-broadcast 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 non-broadcast assumes that there are virtual circuits from every router to every router or fully meshed network. 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.

Point-to-Multipoint Networks

OSPF has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to non-broadcast 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 non-broadcast networks, you must use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Related Commands

Command	Description
ospfv3 cost dynamic default	Configure default metric value to use until metric information is received from the radio.
ospfv3 cost hysteresis	Dampen cost changes.
ospfv3 cost dynamic weight	Amount of impact a link metric change has on the dynamic cost.

outdscp

To specify a DSCP value used for the outbound IP multiplexed superframe for the policy, enter the outdscp command.

outdscp *DSCP_value*

Syntax Description

DSCP_value	DSCP value. Valid values range from 0 to 63. The following DSCP values are also valid:	
	af11	Match packets with AF11 dscp (001010)
	af12	Match packets with AF12 dscp (001100)
	af13	Match packets with AF13 dscp (001110)
	af21	Match packets with AF21 dscp (010010)
	af22	Match packets with AF22 dscp (010100)
	af23	Match packets with AF23 dscp (010110)
	af31	Match packets with AF31 dscp (011010)
	af32	Match packets with AF32 dscp (011100)
	af33	Match packets with AF33 dscp (011110)
	af41	Match packets with AF41 dscp (100010)
	af42	Match packets with AF42 dscp (100100)
	af43	Match packets with AF43 dscp (100110)
	cs1	Match packets with CS1(precedence 1) dscp (001000)
	cs2	Match packets with CS2(precedence 2) dscp (010000)
	cs3	Match packets with CS3(precedence 3) dscp (011000)
	cs4	Match packets with CS4(precedence 4) dscp (100000)
	cs5	Match packets with CS5(precedence 5) dscp (101000)
	cs6	Match packets with CS6(precedence 6) dscp (110000)
	cs7	Match packets with CS7(precedence 7) dscp (111000)
	default	Match packets with default dscp (000000)
	ef	Match packets with EF dscp (101110)

Command Modes

IP multiplexing policy configuration (config-ipmux-policy)

IPv6 multiplexing policy configuration (config-ipmux-policy-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

If you do not enter a value for outdscp, superframes are sent with the DSCP bit set as 0.

Examples

The following example shows how to configure the DSCP value to *10* for the outbound multiplexed superframe in the IPv6 Multiplexing policy *routeRTP-SJ*.

```
router#configure terminal
router(config)#ipv6 mux policy routeRTP-SJ
router(config-ipmux-policy-v6)#outdscp 10
router(config-ipmux-policy-v6)#exit
router(config)#
```

physical-interface

To associate physical interfaces with the VMI on a router, use the **physical-interface** command command in interface-configuration mode. To remove the interface associated interface, use the **no** form of this command.

physical-interface *interface-type/slot*

no physical-interface

Syntax Description

interface-type	Specifies the type of interface or subinterface; value can be Ethernet, Fast Ethernet, or Gigabit Ethernet.
slot	Indicates the slot in which the interface is present.

Command Default

No physical interface exists.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support VMIs in Mobile Ad Hoc Router-to-Radio Networks.

Usage Guidelines

Use the **physical-interface** command to create a physical subinterface.

Only one physical interface can be assigned to a VMI interface. Because a very high number of VMI interfaces can be used, assign a new VMI for each physical interface.

Examples

The following examples shows how to configure the physical interface for vmi1 to FastEthernet0/1.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface wmi1
Router(config-router-if)#physical-interface FastEthernet0/1
Router(config-router-if)#exit
Router(config)#
```

Related Commands

Command	Description
interface vmi	Creates a VMI interface.
mode bypass	Enables VMI to support multicast traffic

router ospfv3

To enter router configuration mode and enable an OSPFv3 routing process to route IPv6 or IPv4 address-family traffic in IPv6 networks, use the **router ospfv3** command in global configuration mode. To terminate an OSPFv3 routing process, use the **no** form of this command.

router ospfv3 *process-id*

no router ospfv3 *process-id*

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.

Defaults

No OSPFv3 routing process is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)GC	This command was introduced.

Usage Guidelines

You can specify multiple IP OSPFv3 routing processes in each router.The **router ospfv3** command must be followed by the **address-family** command for routing of IPv6 traffic to occur.

Each OSPFv3 routing process must have a unique router ID. If a router ID is not configured manually (using the **router-id** *A.B.C.D* command), Cisco IOS attempts to auto-generate a router ID for this process from the IPv4 address of a configured interface. If Cisco IOS cannot generate a unique router-id, the OSPFv3 process remains inactive.

When you use the **no** form of the global **router ospfv3** *process-id* command, the associated interface configuration **ospfv3** *process-id* command is automatically removed from your configuration.

Examples

The following example configures an OSPF routing process and assign a process number of 4:

```
Router(config)# router ospfv3 4
Router(config-router)# router-id 1.1.1.1
Router(config-router)#address-family ipv4 unicast
Router(config-router)#exit
Router(config)#
```

Related Commands

Command	Description
ospfv3 area	Defines the interfaces on which OSPFv3 runs and defines the area ID for those interfaces.

service declassify

To enable the declassification (zeroization) function, enter the **service declassify** command. Use the **no** form of the command to disable the declassification process.

service declassify {erase-flash | erase-nvram | erase-all | erase-default} [trigger GPIO *pin-number*]

[no] service declassify {erase-flash | erase-nvram | erase-all | erase-default} [trigger GPIO *pin-number*]

Syntax Description

erase-flash	Keyword to erase all files in the Flash file system, except the startup configuration, when declassification is invoked.
erase-nvram	Keyword to erase all files in the NVRAM file system when declassification is invoked.
erase-all	Keyword to scrub and erase all files on the router when declassification is invoked
erase-default	Keyword to disable the Flash and NVRAM during the declassify.
trigger GPIO *pin-number*	(Optional) Keyword for the Cisco 5930 ESR to start the declassification at a specific General Purpose Input/Output (GPIO) pin. Valid values range are pins 4, 5, 6, and 7. By default the Cisco 5930 ESR starts declassifying at GPIO pin 4.

Defaults

Declassification(zeroization) is disabled

Command Modes

Global configuration

Command History

Release	Modification
15.2(3)GCA	This command was introduced.

Usage Guidelines

The Cisco 5921 ESR does not support this comand.

The network interfaces are shut down when declassification starts.

The output that appears on the console when declassification starts depends on which options have been configured. It is not possible to document exactly what appears on the screen, because of the complex interactions between the declassification process and the logging process during declassification.

You can use the **trigger GPIO** keyword after any of the other keywords for this command to start the declassification monitoring processing at the specified pin-number. By default the Cisco 5930 ESR starts the declassification monitoring process at GPIO pin 4.

Examples

The following examples show the console output when declassification is invoked.

service declassify erase-all

Caution If you enter the **service declassify erase-all** command, the Flash file system is erased and the Cisco 5930 Flash file system will no longer have a bootable Cisco IOS image. You must initiate error recovery action in order to have a bootable Cisco IOS image.

The startup configuration file is also erased; the router boots from the factory default configuration the next time it is booted.

The output from the **service declassify erase-all** command resembles the following:

```
Router#service declassify erase-all
*Dec 18 01:55:50.043:
Declassification initiated...................................
..........................................................................................
..........................................................................................
..........................................................................................
.............
flashfs[6]: 0 files, 1 directories
flashfs[6]: 0 orphaned files, 0 orphaned directories
flashfs[6]: Total bytes: 129153024
flashfs[6]: Bytes used: 4096
flashfs[6]: Bytes available: 129148928
flashfs[6]: flashfs fsck took 28 seconds.[OK][OK]
*Dec 18 01:56:51.515: %LINK-5-CHANGED: Interface LI-Null0, changed state to
administratively down
*Dec 18 01:56:51.515: %LINK-5-CHANGED: Interface VoIP-Null0, changed state to
administratively down
*Dec 18 01:56:53.607: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
*Dec 18 01:56:55.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface LI-Null0, changed
state to down
*Dec 18 01:56:55.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0, changed
state to down
System Bootstrap, Version 12.4(20120326:184144) [spueblo-post-reg 105], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2012 by cisco Systems, Inc.

Alternate ROM: RSA Signature Verification Passed


DECLASSIFY_DONE FLAG SET

unset Declassify DONE flag.

unset Declassify DONE flag in NVRAM OK

c5930 platform with 1048576 Kbytes of main memory
rommon 1 >
```

service declassify erase-flash

Caution When you enter the **service declassify erase-flash** command, the flash file system is erased and there will not be a bootable image for the router in the Flash file system . Error recovery actions must be initiated to load a bootable image.
The startup configuration file is not erased if you enter the **service declassify erase-flash** command. When the Cisco 5930 ESR is booted, it uses the startup configuration file in NVRAM.

The output from the **service declassify erase-flash** command resembles the following:

```
Router#service declassify erase-flash

*Mar  1 00:01:30.091:
Declassification initiated...
*Mar  1 00:01:34.347: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
*Mar  1 00:01:35.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
System Bootstrap, Version 12.2(1r) [hftseng-MRC_RM 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2002 by cisco Systems, Inc.
C3200 platform with 131072 Kbytes of main memory
rommon 1 >
```

service declassify erase-nvram

Note If you enter the **service declassify erase-nvram** command, the flash file system is not erased. The bootable image in the Flash file system remains and the Cisco 5930 ESR can be booted. The startup configuration file is erased; because the router has no configuration file, it boots from the default configuration.

The output fromthe **service declassify erase-nvram** command resembles the following:

```
Router#service declassify erase-nvram
*Dec 17 17:23:37.303:
Declassification initiated................................
[OK][OK]
*Dec 17 17:23:43.659: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
*Dec 17 17:23:45.867: %LINK-5-CHANGED: Interface LI-Null0, changed state to
administratively down
*Dec 17 17:23:45.867: %LINK-5-CHANGED: Interface VoIP-Null0, changed state to
administratively down
System Bootstrap, Version 12.4(20120326:184144) [spueblo-post-reg 105], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2012 by cisco Systems, Inc.

Alternate ROM: RSA Signature Verification Passed


DECLASSIFY_DONE FLAG SET

unset Declassify DONE flag.

unset Declassify DONE flag in NVRAM OK

c5930 platform with 1048576 Kbytes of main memory
rommon 1 >
```

service declassify erase-default

If you enter the **service declassify erase-default** command, neither the flash file system or NVRAM are erased. The declassification process quickly reaches a state in which the cisco IOS logging process is not operative and the common command output is not seen.

Even though this declassification process shutsdown interfaces, no messages display indication this.

The output fromthe **service declassify erase-default** command resembles the following:

```
Router#service declassify erase-default
*Nov 28 14:24:19.451:
Declassification initiated.................................

System Bootstrap, Version 12.4(20120326:184144) [spueblo-post-reg 105], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2012 by cisco Systems, Inc.

Alternate ROM: RSA Signature Verification Passed


DECLASSIFY_DONE FLAG SET

unset Declassify DONE flag.

unset Declassify DONE flag in NVRAM OK

c5930 platform with 1048576 Kbytes of main memory
rommon 1 >
```

Related Commands

Command	Description
show declassify	Displays the state of the **service declassify** command.

show declassify

To display the state of the zeroization (declassify) function (enabled, in progress, and so forth) and the sequence of declassification steps that will be performed, use the **show declassify** command in global configuration mode.

show declassify

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)GCA	This command was introduced.

Usage Guidelines

The Cisco 5921 ESR does not support this comand.

The output for the **show declassify** command indicates the following things:

- If zeroization (declassification) is enabled
- If zeroization (declassification) is in progress,
- The General Purpose Input/Output (GPIO) pin used as a trigger
- Any optional behaviors that are enabled

The output also shows all actions that will be performed when declassification is initiated.

Examples

The following example shows output for the **show declassify** command:

```
Router# show declassify
Declassify facility: Enabled=Yes  In Progress=No
                     Erase flash=Yes  Erase nvram=Yes
                     Trigger=GPIO
                     GPIO pin: 4
  Obtain memory size
  Shutdown Interfaces
  Declassify Console and Aux Ports
  Erase flash
  Declassify NVRAM
  Declassify RAM, D-Cache, and I-Cache
Router#
```

Table A-1 describes the common fields in the **show declassify** command output.

Table A-1 show declassify Field Descriptions

Field	Description
Enabled	A “Yes” value indicates that zeroization is enabled. A “No” value indicates that zeroization is disabled.
In Progress	A “Yes” value indicates that zeroization is currently in progress. A “No” value indicates that zeroization is currently not in progress.
Erase flash	A “Yes” value indicates that erasure of Flash memory is enabled. A “No” value indicates that the erasure of Flash memory is disabled.
Erase nvram	A “Yes” value indicates that the erasure of NVRAM is enabled. A “No” value indicates that the erasure of NVRAM is disabled.
Trigger	Indicates if a GPIO pin has been configured as a trigger
GPIO pin:	The GPIO pin number set for monitoring to start. The default GPIO pin number is pin 4.
Obtain memory size	Obtain the main memory size in order to understand how much of the memory is to be scrubbed.
Shutdown Interfaces	Shut down any and all network interfaces.
Declassify Console and AUX Ports	Remove potentially sensitive information from console and AUX port FIFOs.
Erase flash	Erase Flash memory.
Declassify NVRAM	Erase NVRAM.
Declassify Communications Processor Module	Erase the memory in the Communications Processor Module (CPM).
Declassify RAM, D-Cache, and I-Cache	Scrub the main memory, erase the Data Cache (D-Cache), and erase the Instruction Cache (I-Cache).

Related Commands

Command	Description
service declassify	Invokes declassification.

show dlep clients

To display router-to-radio peer associations, use the **show dlep clients** command in privileged EXEC mode.

show dlep clients [*interface*] [*peer-id*]

Syntax Description

interface	FastEthernet or VLAN
peer-id	Peer ID with valid range from 1 to 2147483647

Command Modes

Privileged EXEC

Command History

Release	Modification
15.2(4) GC	This command was introduced.

Usage Guidelines

Use the **show dlep clients** command to display router-to-radio peer associations.

Examples

The following example shows how to display router-to-radio peer associations on all interfaces:

```
Router# show dlep clients

DLEP Clients for all interfaces:


DLEP Clients for Interface FastEthernet0/1
DLEP Server IP=12.12.12.101:55555 Sock=1

DLEP Client IP=12.12.12.7:38681
 Peer ID=1, Virtual template=1
 Description: DLEP_Radio_Sim_1
 Peer Timers (all values in seconds):
  Heartbeat=10, Dead Interval=40, Terminate ACK=10
 Neighbor Timers (all values in seconds):
  Activity timeout=0, Neighbor Down ACK=10
```

Related Commands

Command	Description
show dlep config	Displays the DLEP server configuration.
show dlep neighbors	Displays neighbor sessions on the specified interface.

show dlep config

To display the DLEP server configuration, use the **show dlep config** command in privileged EXEC mode.

show dlep config *interface*

Syntax Description

interface	FastEthernet or VLAN

Command Modes

Privileged EXEC

Command History

Release	Modification
15.2(4) GC	This command was introduced.

Usage Guidelines

Use the **show dlep config** command to display the DLEP server configuration.

Display DLEP server configuration example

The following example shows how to display the DLEP server configuration:

```
Router# show dlep config
DLEP Configuration for FastEthernet0/1

DLEP Server IP=12.12.12.101:55555
 Virtual template=1
 Timers (all values are in seconds):
 Missed heartbeat threshold=4, Peer Terminate ACK timeout=10
 Neighbor activity timeout=0, Neighbor Down ACK timeout=10
```

Related Commands

Command	Description
show dlep clients	Displays router-to-radio peer associations.
show dlep neighbors	Displays neighbor sessions on the specified interface.

show dlep counters

To display DLEP counters, use the **show dlep counters** command in privileged EXEC mode.

show dlep counters [*vmi-interface*]

Syntax Description

vmi-interface	(Optional) Interface where DLEP is configured.

Command Default

If no arguments are specified, counters on all VMI interfaces with DLEP configured are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Examples

The following is example output from the **show dlep counters** command used to display input and output DLEP counts on the gigabitEthernet interface:

```
Router# show dlep counters gigabitEthernet 0/1.5

Peer Counters:
 RX Peer Discovery     0      TX Peer Offer             0
 RX Heartbeat          22     TX Heartbeat              22
 RX Peer Terminate     0      TX Peer Terminate Ack     0
 RX Peer Terminate Ack 0      TX Peer Terminate         0

Neighbor Counters:
 RX Neighbor Up        0      TX Neighbor Up Ack        0
 RX Metric             27
 RX Neighbor Down      0      TX Neighbor Down Ack      0
 RX Neighbor Down Ack  0      TX Neighbor Down          0

Exception Counters:
 RX Invalid Message    0      RX Unknown Message        0
 Pre-Existing Neighbor 0      Neighbor Resource Error   0
 Neighbor Not Found    0      Neighbor Msg Peer Not Up  0

Timer Counters:
 Peer Heartbeat Timer         22
 Peer Terminate Ack Timer     0
 Neighbor Terminate Ack Timer 0
 Neighbor Activity Timer      0

Router#
```

Table A-2 describes the significant count definitions in the **show dlep counters** command display.

Table A-2 show dlep counters Count Definitions

Count	**Definition**
Peer Counter	
RX Peer Discovery	Number of receive Peer Discovery messages.
TX Peer Offer	Number of transmit Peer Offer messages.
RX Heartbeat	Number of receive Heartbeat messages.
TX Heartbeat	Number of transmit Heartbeat messages.
RX Peer Terminate	Number of receive Peer Terminate messages.
TX Peer Terminate Ack	Number of transmit Peer Terminate acknowledgement messages.
RX Peer Terminate Ack	Number of receive Peer Terminate acknowledgement messages.
TX Peer Terminate	Number of transmit Peer Terminate messages.
Neighbor Counter	
RX Neighbor Up	Number of receive Neighbor Up messages.
TX Neighbor Up Ack	Number of transmit Neighbor Up acknowledgement messages.
RX Metric	Number of receive Metric messages.
RX Neighbor Down	Number of receive Neighbor Down messages.
TX Neighbor Down Ack	Number of transmit Neighbor Down acknowledgement messages.
RX Neighbor Down Ack	Number of receive Neighbor Down acknowledgement messages.
TX Neighbor Down	Number of transmit Neighbor Down messages.
Exception Counters	
RX Invalid Message	Number of messages received of a type not expected.
RX Unknown Message	Number of messages received of unknown type.
Preexisting Neighbor	Number of messages received on a preexisting neighbor.
Neighbor Resource	Number of resource errors during a neighbor operation.
Neighbor Not Found	Number of messages received for a non-existent neighbor.
Neighbor Msg Peer Not Up	Number of neighbor messages received when the peer state was down.
Timer Counters	
Peer Heartbeat Timer	Number of timer expirations for Peer Heartbeat.
Peer Terminate Ack Timer	Number of timer expirations for Peer Terminate acknowledgement.
Neighbor Terminate Ack Timer	Number of timer expirations for Neighbor Terminate acknowledgements.
Neighbor Activity Timer	Number of timer expirations for Neighbor Activity.

show dlep neighbors

To display neighbor sessions on the specified interface, use the **show dlep neighbors** command in privileged EXEC mode.

show dlep neighbors *interface*

Syntax Description

interface	FastEthernet or VLAN

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)GC	This command was introduced.

Usage Guidelines

Use the **show dlep neighbors** command to display the established neighbor sessions.

Display neighbors example

The following example shows how to display the established neighbor sessions on all interfaces:

```
Router# show dlep neighbors

DLEP Neighbors for all interfaces:

DLEP Neighbors for Interface FastEthernet0/1
DLEP Server IP=12.12.12.101:28672 Sock=1

  Global Session ID=101
 MAC Address: 1122.3344.5566
 Vlan ID: 0
 Metrics:  rlq=100  resources=100  latency=10 milliseconds
           cdr=100000 Kbps  mdr=100000 Kbps
```

Related Commands

Command	Description
show dlep clients	Displays router-to-radio peer associations.
show dlep config	Displays the DLEP server configuration.

show ip eigrp neighbors

To display 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** | **detail**]

Syntax Description

interface-type	(Optional) Filters that output by interface.
as-number	(Optional) Filters that output by autonomous system number.
static	(Optional) Keyword to display static routes.
detail	(Optional) Keyword to display detailed neighbor information.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0(7)T	The static keyword was added.
12.2(15)T	Support for NSF restart operations was integrated into the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show ip eigrp neighbors** command to determine when neighbors become active and inactive. The **show ip eigrp neighbors** command is also useful for debugging certain types of transport problems.

Examples

The following is example output from the **show ip eigrp neighbors** command:

```
Router# show ip eigrp neighbors
P-EIGRP Neighbors for process 77
Address                Interface     Holdtime Uptime   Q      Seq  SRTT  RTO
                                     (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28           Ethernet1     13       0:00:41  0      11   4     20
172.16.80.28           Ethernet0     14       0:02:01  0      10   12    24
172.16.80.31           Ethernet0     12       0:02:02  0      4    5     20
```

show ip mux

To display configured IP multiplexing statistics, use the **show ip mux** command in user EXEC or privileged EXEC mode.

show {**ip** | **ipv6**} **mux**

Syntax Description

ip	Keyword to specify IPv4 multiplexing
ipv6	Keyword to specify IPv6 multiplexing

Command Modes

User Exec

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Examples

The following example shows how to display IP multiplex statistics.

```
router#show ip mux
IPv4 Multiplexing
  Superframe UDP Port: 6682

Multiplexing Policies
 muxpol             Outbound DSCP:      19
                    Match DSCP values:  af21 19
 muxpol2            Outbound DSCP:      af11
                    Match DSCP values:  11
 muxpol3            Outbound DSCP:      2
                     Match DSCP values: 1

IPv4 Multiplex Cache Statistics
  Current Entries:                3
  Maximum Number of Entries:      56818
  Cache High Water Mark:          3
  Total Stale Entries:            0
  Total Do-Not-Multiplex Entries: 0
router#
```

Table A-3 describes the significant fields of the **show ip mux** command output.

Table A-3 Description of show ip mux Output

Field	Description
Superframe UDP Port:	UDP port configured for IP multiplexing.
Multiplexing Policies	List of each configured IP multiplexing policy with the policy name, configured outbound DSCP value and DSCP values in packets bound for multiplexing.
Current Entries	Number of entries listed in the IP multiplex cache.

Table A-3 Description of show ip mux Output

Field	Description
Maximum Number of Entries	Maximum number of entries that the cache can contain.
Cache High Water Mark	Maximum number of entries that have ever been in the cache at one time. This value may not represent the current number of entries in the cache.
Total Stale Entries	An entry in the cache that is older than 30 seconds and has not been referenced. Every 30 seconds, any unreferenced entry older that 30 seconds are marked stale and stale entries are deleted from the cache. If the cache is full, stale entries are overwritten first.
Total Do-Not-Multiplex Entries	Number of entries in the cache designated to not multiplex

show ip mux cache

To display cache statistics, use the **show ip mux cache** command in user EXEC or privileged EXEC mode.

show {**ip** | **ipv6**} **mux cache** [**profile** *profile_name* | **nomux** | **stale**]

Syntax Description

ip	Keyword to specify IPv4 multiplexing
ipv6	Keyword to specify IPv6 multiplexing
profile *profile_name*	Keyword and profile name to show IP multiplex cache contents by profile
nomux	Keyword to display IP multiplex cache of do not multiplex entries
stale	Keyword to display IP multiplex cache stale entries

Command Modes

User Exec

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Examples

The following example shows how to display the cache statistics.

```
router#show ipv6 mux cache

IPv6 Multiplex Cache Statistics

Current Entries:                  2
  Maximum Number of Entries:      9615
  Cache High Water Mark:          2
  Total Stale Entries:            0
  Total Do-Not-Multiplex Entries: 2

IPv6 Multiplex Cache Contents

Destination Address                        Port      Protocol     DSCP      Profile
--------------------------------------------------------------------------------
200:200:200:200:200:0:E01:5600             0         UDP          1         r1v6
200:200:200:200:200:0:E01:5600             0         UDP          af11      No mux
router#
```

Table A-4 describes the significant fields of the **show ip mux cache** command output.

Table A-4 Description of show ip mux cache profile Output

Field	Description
Current Entries	Number of entries listed in the IP multiplex cache.
Maximum Number of Entries	Maximum number of entries that the cache can hold

Table A-4 Description of show ip mux cache profile Output

Field	Description
Cache High Water Mark	Maximum number of entries that have ever been stored in the cache. If this value varies greatly from the maximum number of cache entries, you may want to consider changing the cache size.
Total Stale Entries	An entry in the cache that is older than 30 seconds and has not been referenced. Every 30 seconds, any unreferenced entry older that 30 seconds are marked stale and stale entries are deleted from the cache. If the cache is full, stale entries are overwritten first.
Total Do-Not-Multiplex Entries	Number of entries in the cache designated to not multiplex
Destination Address	Destination IPv4 or IPv6 address for the cache entry
Port	Port configured for the cache entry
Protocol	Protocol configured for the cache entry
DSCP	Differentiated Services Control Point
Profile	Name of the profile

The following example shows how to display the cache statistics for do-not-multiplex entries:

```
router#show ip mux cache nomux

IPv4 Multiplex Cache

Destination Address    Port    Protocol    DSCP    Profile
-----------------------------------------------------------
1.1.2.1                0       ICMP        0       No mux
router#
```

The following example shows how to display the cache statistics for stale entries:

```
router#show ip mux cache stale

IPv4 Multiplex Cache

Destination Address    Port    Protocol    DSCP    Profile
-----------------------------------------------------------
20.20.20.21            1000    UDP         1       r1 (stale)
20.20.20.21            1000    UDP         af12    r1 (stale)
router#
```

The following example shows how to display the cache statistics for the IP multiplexing profile r1.

```
Router#show ip mux cache profile r1

IPv4 Multiplex Cache

Destination Address    Port    Protocol    DSCP    Profile
-----------------------------------------------------------
20.20.20.20            0       ICMP        0       r1
20.20.20.21            1000    UDP         1       r1 (stale)
20.20.20.21            1000    UDP         af12    r1 (stale)
20.20.20.20            1001    UDP         af21    r1
Router#
```

show ip mux interface

To display configured IP multiplexing statistics for an interface, use the **show ip mux interface** command in user EXEC or privileged EXEC mode.

show {**ip** | **ipv6**} **mux interface** *interface_type*

Syntax Description

ip	Keyword to specify IPv4 multiplexing
ipv6	Keyword to specify IPv6 multiplexing
interface_type	Interface type. The following interface types are valid: • Ethernet: IEEE 802.3 • Tunnel: Tunnel interface • Virtual-Template: Virtual Template interface • vmi: Virtual Multipoint Interface

Command Modes

User Exec

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

If you do not specify an interface type, the show ip mux interface commands displays statistics for all interfaces with IP multiplexing configured.

Examples

The following example shows how to display IP multiplex statistics for Ethernet 0/1.

```
router#show ip mux interface Ethernet0/1
IP multiplexing statistics for Ethernet0/1:
  Transmit:
   IPv4 superframes transmited: 20430
   IPv4 packets multiplexed:    30555
   Average TX mux ratio:        1.49:1
  Receive:
   IPv4 superframes received:   22009
   IPv4 packets demuxed:        32634
   IPv4 format errors:          0
   Average RX mux ratio:        1.48:1
router#
```

Table A-5 describes the significant fields of the **show ip mux interface** command output.

Table A-5 Description of show ip mux interface Output

Field	Description
IPv4 super frames transmitted	Number of IPv4 superframes transmitted from the interface
IPv4 packets multiplexed	Number of packets that have been processed and put into superframes
Average TX mux ratio	Ratio of the total number of packets put into superframes divided by the number of superframes transmitted
IPv4 super frames received	Number of IPv4 superframes received over the interface
IPv4 packets demuxed	Number of IPv4 packets demultiplexed from received superframes
IPv4 format errors	Number of packets with format errors after they have been demultiplexed
Average RX mux ratio	Ratio of the total number of successfully demultipluxed packets divided by the number of superframes received

show ip mux profile

To display cache statistics for a specific IP multiplexing profile, use the **show ip mux cache profile** command in user EXEC or privileged EXEC mode.

show {**ip** | **ipv6**} **mux profile** *profile_name*

Syntax Description

ip	Keyword to specify IPv4 multiplexing
ipv6	Keyword to specify IPv6 multiplexing
profile_name	Name of the IP multiplexing profile

Command Modes

User Exec

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

If you do not specify a *profile_name*, the this command displays the statistics for all configured profiles.

Examples

The following example shows how to display the cache statistics for the IPv6 profile r1v6.

```
router#show ipv6 mux profile rlv6
Profile r1v6
  Shutdown:                    No
  Destination:                 2000:0:1:2:A8BB:CCFF:FE01:5610
  Source:                      2000:0:1:1:A8BB:CCFF:FE01:5510  (Ethernet0/1)
  Access-list:                 muxv6acl
  TTL:                         64
  Max mux length:              1452
  MTU:                         1500
  Hold time(ms):               20
  Single packet superframes:   Enabled

  Inbound (demux) Statistics
    Superframes received:         0
    Packets demultiplexed:        0
    Avg. Inbound Multiplex ratio: N/A

  Outbound (mux) Statistics
  Default Policy
    Packets: 0/0  Full Superframes: 0  Partial Superframes: 0
    Avg. Outbound Multiplex ratio: N/A     Mux length exceeded: 0

  Policy dscp4
    Packets: 3963/3616  Full Superframes: 0  Partial Superframes: 984
    Avg. Outbound Multiplex ratio: 3.67:1     Mux length exceeded: 0

router#
```

Table A-6 describes the significant fields of the **show ipv6 mux profile** command output.

Table A-6 Description of show ip mux profile Output

Field	Description
Profile	Name of the configured IP multiplexing profile and the current state of IP multiplexing for the profile: either **enabled** or **disabled**
Shutdown	Current state of the profile. Shutdown = No, then the profile is enabled. Shutdown = Yes, then the profile is disabled.
Destination	Destination IPv4 or IPv6 address configured for the profile
Source	Source IPv4 or IPv6 address configured for the profile
Access-list	Name of the access-list used by the IP multiplexing profile
TTL	Configured time-to-live (TTL) value for outbound superframes. Number of hops before the superframe expires
Max mux length	Maximum packet size that the multiplex profile can hold for multiplexing
MTU	Maximum transmission unit (MTU) size for an outbound superframe
Holdtime (ms)	Length of time IP multiplexing waits having not received a packet before sending the superframe
Single packet superframes	**Enabled** means that superframes with only one packet are sent. **Disabled** means that single packets are not sent as superframes.
Inbound (demux) Statistics	
Superframes received	Number of superframes the IP multiplex policy has received
Packets demultiplexed	Number of packets that have been demultiplexed from superframes
Avg. Inbound Multiplex ratio	Number of inbound packets demultiplexed divided by the number of superframes received
Outbound (mux) Statistics, listed by policy name	
Packets	The first value is the number of outbound packets processed by the policy. The second value is the number of packets that were transmitted inside superframes.
Full Superframes	Number of full superframes that the policy has sent
Partial Superframes	Number of partial superframes the policy has sent

Table A-6 Description of show ip mux profile Output

Field	Description
Avg. Outbound Multiplex ratio	Ratio of the number of packets processed by the policy divided by the number of full superframes and partial superframes sent by the policy
Mux length exceeded	Number of packets processed by the policy that exceed the configured maximum packet length

show ip redirects

To display the address of a default gateway (router) and the address of hosts for which an ICMP redirect message has been received, use the **show ip redirects** command in user EXEC or privileged EXEC mode.

show ip redirects

Command Modes

User EXEC

Privileged EXEC

Command History

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

Usage Guidelines

This command displays the default router (gateway) as configured by the **ip default-gateway** command.

The **ip mtu** command enables the router to send ICMP redirect messages.

Examples

The following is example output from the show ip redirects command:

```
Router# show ip redirects
Default gateway is 172.16.80.29
Host               Gateway           Last Use    Total Uses  Interface
172.16.1.111      172.16.80.240        0:00          9       Ethernet0
172.16.1.4        172.16.80.240        0:00          4       Ethernet0
```

Related Commands

Command	Description
ip default-gateway	Defines a default gateway (router) when IP routing is disabled.
ip mtu	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.

show ipv6 eigrp neighbors

To display the neighbors discovered by EIGRP for IPv6, use the **show ipv6 eigrp neighbors** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp neighbors [*interface-type* | *as-number* | **static** | **detail**]

Syntax Description

interface-type	(Optional) Interface type.
as-number	(Optional) Autonomous system number.
static	(Optional) Keyword to display static routes.
detail	(Optional) Keyword to display detailed neighbor information.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the show ipv6 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 example output from the **show ipv6 eigrp neighbors** command:

```
Router# show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 1
H Address                  Interface      Hold      Uptime     SRTT     RTO   Q     Seq
                                          (sec)                (ms)           Cnt   Num
0 Link-local address:         Et0/0        14       00:00:13    11      200   0      2
FE80::A8BB:CCFF:FE00:200
```

show ospfv3

To display information about one or more OSPFv3 routing processes, use the **show ospfv3** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(2)GC	The syntax for the command changed from **show IPv6 OSPF** to **show ospfv3**. This output for this command was expanded to include IPv4 and IPv6 address family information.

Examples

The following is example output from the **show ospfv3** command:

```
Router# show ospfv3 100
 Routing Process "ospfv3 100" with ID 5.5.5.5
 Supports IPv4 Address Family
 Supports Link-local Signaling (LLS)
 It is an autonomous system boundary router
 Redistributing External Routes from,
 connected
 SPF schedule delay 1 secs, Hold time between two SPFs 1 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 2. Checksum Sum 0x01C812
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Reference bandwidth unit is 100 mbps
 Relay willingness value is 128
 Pushback timer value is 2000 msecs
 Relay acknowledgement timer value is 1000 msecs
 LSA cache Enabled : current count 0, maximum 1000
 ACK cache Enabled : current count 0, maximum 1000
 Selective Peering is enabled per node
 Redundancy level: 1
 Peering delay timer: 250 msecs
 Hello requests and responses will be sent multicast
    Area BACKBONE(0)
        Number of interfaces in this area is 4
        SPF algorithm executed 13 times
        Number of LSA 6. Checksum Sum 0x0208A7
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

show ospfv3 database

To display the contents of the OSPFv3 Link State Advertisement (LSA) database, or selective parts thereof, use the **show ospfv3 database** command in privileged EXEC mode. The various forms of this command deliver information about different OSPF LSAs.

show ospfv3 [*process-id*] [*area-id*] **database**

show ospfv3 [*process-id*] [*area-id*] **database** [**adv-router** [*router-id*]]

show ospfv3 [*process-id*] [*area-id*] **database** [**database-summary**]

show ospfv3 [*process-id*] [*area-id*] **database** [**external** [*link-state-id*] [**adv-router** | **internal** | **self-originate**] [*ipv6-address*]]

show ospfv3 [*process-id*] [*area-id*] **database** [**inter-area prefix** [*link-state-id*] [**adv-router** | **internal** | **self-originate**] | [*ipv6-address*]]

show ospfv3 [*process-id*] [*area-id*] **database** [**inter-area router** [*link-state-id*] [**adv-router** | **internal** | **self-originate**] | [*destination-router-id*]]

show ospfv3 [*process-id*] [*area-id*] **database** [**link**] [*link-state-id*] [**adv-router** | **internal** | **self-originate**] [**interface** [*interface-name*]]

show ospfv3 [*process-id*] [*area-id*] **database** [**network**] [*link-state-id*] [**adv-router** | **internal** | **self-originate**]

show ospfv3 [*process-id*] [*area-id*] **database** [**nssa-external** [*link-state-id*] [**adv-router** | **internal** | **self-originate**] | [*ipv6-address*]]

show ospfv3 [*process-id*] [*area-id*] **database** [**prefix**] [*link-state-id*] [**adv-router** | **internal** | **self-originate**] [**router** | **network**]

show ospfv3 [*process-id*] [*area-id*] **database** [**promiscuous**]

show ospfv3 [*process-id*] [*area-id*] **database** [**router**] [**adv-router** | **internal** | **self-originate**] [*link-state-id*]

show ospfv3 [*process-id*] [*area-id*] **database** [**self-originate**] [*link-state-id*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
area-id	(Optional) Displays information only about a specified area of the database.
adv-router [*router-id*]	(Optional) Keyword to display all the LSAs of the specified router. This argument must be in the form documented in RFC 2740 where the address is specified in hexadecimal using 16-bit values between colons.
database-summary	(Optional) Keyword to display how many of each type of LSA for each area there are in the database, and the total.

external	(Optional) Keyword to display information only about the external LSAs.
link-state-id	(Optional) An integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
internal	(Optional) Keyword to display internal LSA information.
self-originate	(Optional) Keyword to display only self-originated LSAs (from the local router).
ipv6-address	(Optional) Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
destination-router-id	(Optional) The specified destination router ID.
inter-area prefix	(Optional) Keyword to display information only about LSAs based on inter-area prefix LSAs.
inter-area router	(Optional) Keyword to display information only about LSAs based on inter-area router LSAs.
link	(Optional) Keyword to display information about the link LSAs.
interface	(Optional) Keyword to display information about the LSAs filtered by interface context.
interface-name	(Optional) Specifies the LSA interface.
network	(Optional) Keyword to display information only about the network LSAs.
nssa-external	(Optional) Keyword to display information only about the not so stubby area (NSSA) external LSAs.
prefix	(Optional) Keyword to display information on the intra-area-prefix LSAs.
promiscuous	(Optional) Keyword to display temporary LSAs in a MANET environment.
ref-lsa {**router** | **network**}	(Optional) Keyword to display further filters the prefix LSA type.
router	(Optional) Keyword to display information only about the router LSAs.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced as **show ipv6 OSPF database**.
12.4(24)GC	The promiscuous keyword was added.
15.1(2)GC	The syntax for the command changed from **show IPv6 OSPF database** to **show ospfv3 database**. The output for this command was expanded to include IPv4 and IPv6 address family information.

Usage Guidelines

The **adv-router** keyword requires a router ID. The **self-originate** keyword displays only those LSAs that originated from the local router. Both of these keywords can be appended to all other keywords used with the **show ospfv3 database** command to provide more detailed information.

Examples

The following is example output from the **show ospfv3 database** command when no arguments or keywords are used:

```
Router# show ospfv3 database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#          Prefix
172.16.4.4         249         0x80000001    FEC0:3344::/32
172.16.4.4         219         0x80000001    FEC0:3366::/32
172.16.6.6         247         0x80000001    FEC0:3366::/32
172.16.6.6         193         0x80000001    FEC0:3344::/32
172.16.6.6         82          0x80000001    FEC0::/32

            Inter Area Router Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

Table A-7 describes the significant fields shown in the display.

Table A-7 show ospfv3 database Field Descriptions

Field	Description
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Link ID	Interface ID number.
Ref-lstype	Referenced link-state type.
Ref-LSID	Referenced link-state ID.

show ospfv3 flood-list

To display a list of OSPFv3 LSAs waiting to be flooded over an interface, use the **show ospfv3 flood-list** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] **flood-list** *interface-type interface-number*

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
interface-type	Interface type over which the LSAs will be flooded.
interface-number	Interface number over which the LSAs will be flooded.

Command Modes

User EXEC

Command History

Release	Modification
12.4(24)GC	This command was introduced.
15.1(2)GC	The syntax for the command changed from **show IPv6 OSPF flood-list** to **show ospfv3 flood-list**. This output for this command was expanded to include IPv4 and IPv6 address family information.

Usage Guidelines

Use this command to display OSPF packet pacing.

Examples

The following is example output from the **show ospfv3 flood-list** command:

```
Router# show ospfv3 flood-list

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031   0       0x1971

 Interface FastEthernet0/0, Queue length 0

 Interface ATM3/0, Queue length 0
Router#
```

Table A-8 describes the significant fields shown in the display.

Table A-8 show ospfv3 flood-list Field Descriptions

Field	Description
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)	Identification of the router for which information is displayed.
Interface POS4/0	Interface for which information is displayed.
Queue length	Number of LSAs waiting to be flooded.
Link state retransmission due in	Length of time before next link-state transmission.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ospfv3 interface

To display OSPF-related interface information, use the **show ospfv3 interface** command in privileged EXEC mode.

show ospfv3 [*process-id*] **interface** [*interface-type interface-number*] [**brief**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
interface-type interface-number	(Optional) Interface type and number.
brief	(Optional) Keyword to display brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)GC	The syntax for the command changed from **show IPv6 OSPF interface** to **show ospfv3 interface**. This output for this command was expanded to include IPv4 and IPv6 address family information.

Examples

The following is example output from the **show ospfv3 interface** command:

```
Router# show ospfv3 interface

Ethernet0/0 is up, line protocol is up
 Link Local Address FE80::A8BB:CCFF:FE01:5500, Interface ID 3
 Area 0, Process ID 100, Instance ID 0, Router ID 172.16.3.3
 Network Type MANET, Cost: 10 (dynamic), Cost Hysteresis: Disabled
 Cost Weights: Throughput 100, Resources 100, Latency 100, L2-factor 100
 Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
 Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
   Hello due in 00:00:01
 Supports Link-local Signaling (LLS)
 Index 1/1/1, flood queue length 0
 Next 0x0(0)/0x0(0)/0x0(0)
 Last flood scan length is 2, maximum is 2
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 2.2.2.2
 Suppress hello for 0 neighbor(s)
 Incremental Hello is enabled
 Local SCS number 1
 Relaying enabled
Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
Router#
```

Table A-9 describes the significant fields shown in the display.

Table A-9 show ospfv3 interface Field Descriptions

Field	Description
Ethernet0/0	Status of the physical link and operational status of protocol.
Link Local Address	Interface IPv6 address.
Area 0, Process ID 100, Instance ID 0, Router ID 172.16.3.3	The area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type MANET, Cost: 10 (dynamic), Cost hysteresis: Disabled	Network type and link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Timer intervals configured	Configuration of timer intervals, including hello-increment and dead-interval.
Hello due in 00:00:01	Number of seconds until the next hello packet is sent out this interface.
Supports Link-local Signaling (LLS)	Indicates that LLS is supported.
Last flood scan length is 2, maximum is 2	Indicates length of last flood scan and the maximum length.
Last flood scan time is 0 msec, maximum is 0 msec	Indicates how many milliseconds the last flood scan occurred and the maximum time length.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.
Adjacent with neighbor 2.2.2.2	Lists the adjacent neighbor.
Suppress hello for 0 neighbor(s)	Indicates the number of neighbors to suppress hello messages.

show ospfv3 neighbor

To display OSPF neighbor information on a per-interface basis, use the **show ospfv3 neighbor** command in privileged EXEC mode.

The **show ospfv3 neighbor** command without the process-id displays OSPFv3 neighbor information for both IPv4 and IPv6 address families for all OSPFv3 processes.

show ospfv3 [*process-id*] **neighbor** [interface-*type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled.The range is 1 to 65535.
interface-type interface-number	(Optional) Interface type and number.
neighbor-id	(Optional) Neighbor ID.
detail	(Optional) Keyword to display all neighbors in detail (lists all neighbors).

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)GC	The syntax for the command changed from **show IPv6 OSPF neighbor** to **show ospfv3 neighbor**. This output for this command was expanded to include IPv4 and IPv6 address family information.

Examples

The following is example output from the **show ospfv3 neighbor** command:

```
Router# show ospfv3 neighbor

OSPFv3 Router with ID (42.1.1.1) (Process ID 42)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
44.4.4.4        1    FULL/  -        00:00:39           12            vm1

OSPFv3 Router with ID (1.1.1.1) (Process ID 100)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
4.4.4.4          1   FULL/  -        00:00:35           12            vm1
```

The following is example output from the **show ospfv3 neighbor** command with the **detail** keyword:

```
Router# show ospfv3 neighbor detail
Neighbor 42.4.4.4, interface address 4.4.4.4
     In the process ID 42 area 0 via interface vmi1
Neighbor: interface-id 12, link-local address FE80::A8BB:CCFF:FE01:5800
     Neighbor priority is 1, State is FULL, 6 state changes
     Options is 0x000F12 in Hello (E-Bit, R-bit, AF-Bit, L-Bit, I-Bit, F-Bit)
     Options is 0x000112 in DBD (E-Bit, R-bit, AF-Bit)
     Dead timer due in 00:00:33
     Neighbor is up for 00:09:43
     Index 1/1/1, retransmission queue length 0, number of retransmission 0
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 0, maximum is 0
     Last retransmission scan time is 0 msec, maximum is 0 msec
     Neighbor is incremental Hello capable
     Last known SCS number 1
     Neighbor's willingness 128
     We are standby relay for the neighbor
     This neighbor is standby relay for us
     Neighbor is running Manet Version 10
Neighbor 4.4.4.4
      In the process ID 100 area 0 via interface vmi1
Neighbor: interface-id 12, link-local address FE80::A8BB:CCFF:FE01:5800
     Neighbor priority is 1, State is FULL, 6 state changes
     Options is 0x000E13 in Hello (V6-Bit, E-Bit, R-bit, L-Bit, I-Bit, F-Bit)
     Options is 0x000013 in DBD (V6-Bit, E-Bit, R-bit)
     Dead timer due in 00:00:37
     Neighbor is up for 00:09:43
     Index 1/1/1, retransmission queue length 0, number of retransmission 0
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 0, maximum is 0
     Last retransmission scan time is 0 msec, maximum is 0 msec
     Neighbor is incremental Hello capable
     Last known SCS number 1
     Neighbor's willingness 128
Two-hop neighbors:
     5.5.5.5
     We are standby relay for the neighbor
     This neighbor is active relay for us
     Neighbor is running Manet Version 10
     Selective Peering is enabled
     1 paths to this neighbor
Neighbor peering state: Slave, local peering state: Master,
     Default cost metric is 0
     Minimum incremental cost is 10
```

Table A-10 describes the significant fields shown in the display.

Table A-10 show ospfv3 neighbor Field Descriptions

Field	Description
Neighbor ID; Neighbor	Neighbor router ID.
In the area	Area and interface through which the OSPF neighbor is known.
Pri; Neighbor priority	Router priority of the neighbor, neighbor state.
State	OSPF state.
State changes	Number of state changes since the neighbor was created.
Options	Hello packet options field contents. (E-bit only. Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)
Dead timer due in	Expected time before Cisco IOS software will declare the neighbor dead.

Table A-10 show ospfv3 neighbor Field Descriptions (continued)

Field	Description
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into two-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in the retransmission queue.
number of retransmission	Number of times update packets have been resent during flooding.
First	Memory location of the flooding details.
Next	Memory location of the flooding details.
Last retransmission scan length	Number of link state advertisements (LSAs) in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build last retransmission packet.
maximum	Maximum time taken to build any retransmission packet.
Neighbor is incremental Hello capable	The MANET neighbor interface is capable of receiving increment Hello messages. A neighbor must be capable of sending and receiving incremental Hello packets to be a full neighbor on a MANET interface.
Last known SCS number 1	Indicates the last received MANET state. The State Change Sequence number is included in the incremental Hello packet.
Neighbor’s willingness 128	Indicates the neighbors willingness to act as an Active Relay for this router, on a scale of 0 (not willing) to 255 (always willing). Willingness is used as a tiebreaker when electing an Active Relay.
We are standby relay for neighbor	Indicates that this router will not flood LSAs received from this neighbor until one or more of our neighbors fails to acknowledge receiving the LSA flood from another neighbor.
Neighbor is running Manet Version 10	Indicates Manet Version number. Routers cannot establish full adjacency unless they are running the same Manet Version.
Two-hop neighbors	Lists the router-ids of all full neighbors of the specified router that are not also neighbors of this router.
Selective Peering is enabled	The MANET interface has selective peering enabled.

Table A-10 show ospfv3 neighbor Field Descriptions (continued)

Field	Description
1 paths to this neighbor	Indicates the number of unique paths to this router that exist in the routing table. This number may exceed the redundancy level configured for this OSPFv3 process.
Neighbor peering state...	Indicates which router is entitled to make the selective peering decision. Generally speaking, the entitled router has the smaller number of full neighbors at the time the routers discover each other.
Default cost metric is 0	Indicates the maximum OSPF cost to a new neighbor in order to be considered for selective peering. If 0, a_threshold OSPF cost is not required for consideration.
Minimum incremental cost is 10	Indicates the minimum cost increment for the specified interface.

show ospfv3 neighbor manet

To display OSPF neighbor information, use the **show ospfv3 neighbor manet** command in privileged EXEC mode.

The **show ospfv3 neighbor manet** command displays manet neighbor information.

show ospfv3 [*process-id*] [*area-id*] **neighbor manet**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here may be assigned administratively when OSPF routing is enabled. Valid values range from 1 to 65535.
area-id	(Optional) Identifier to display information about a specified area of the database.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)GC	This command was introduced.
15.1(2)GC	This output for this command was expanded to include IPv4 and IPv6 address family information.

Examples

The following is example output from the **show ospfv3 neighbor manet** command:

```
Router# show ospfv3 neighbor manet

            OSPFv3 Router with ID (4.4.4.4) (Process ID 4)

Area BACKBONE(0) (Inactive)
Codes: D - cost dynamic default, R - received link cost,
       I - inherited from interface

Neighbor ID       State  Nbr Relay    Cost        Interface
 2.2.2.2           FULL      -      10   (I)      Ethernet0/0
```

show ospfv3 promiscuous acknowledgments

To display the cache of temporary acknowledgments, use the **show ospfv3 promiscuous acknowledgments** command in privileged EXEC mode.

show ospfv3 [*process-id*] **promiscuous acknowledgments** [**detail**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled. The range is 1 to 65535.
detail	(Optional) Keyword to display all neighbors in detail (lists all neighbors).

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)GC	The syntax for the command changed from **show IPv6 OSPF promiscuous acknowledgements** to **show ospfv3 promiscuous acknowledgements**. This output for this command was expanded to include IPv4 and IPv6 address family information.

Examples

The following is example output from the **show ospfv3 promiscuous acknowledgments** command using the **detail** keyword. It The shows that the cache of temporary acknowledgements is not allocated for the router.

```
Router# show ospfv3 promiscuous acknowledgements detail


        OSPFv3 Router with ID (5.5.5.5) (Process ID 100), (Area 0)


Type   LS ID           ADV RTR         Seq#        Age  Scope
0x4005 2               7.7.7.7         0x80000001  114  AS
    Ack received from the following router-ids:
    1.1.1.1
0x4005 8               7.7.7.7         0x80000002  2    AS
    Ack received from the following router-ids:
    7.7.7.7          4.4.4.4          6.6.6.6          1.1.1.1
0x4005 10              7.7.7.7         0x80000002  2    AS
    Ack received from the following router-ids:
    7.7.7.7          4.4.4.4          6.6.6.6          1.1.1.1
Router#
```

Related Commands

Command	Description
show ospfv3 database	Displays lists of information related to the OSPF database for a specific router.

show pppoe

To display information about active PPPoE neighbor sessions, use the **show pppoe** command in privileged EXEC mode.

show pppoe {**derived** *group* | **relay** [**context all**] | **session** [**all** | *interface* | **packets**] | **summary** | **throttled mac**}

Syntax Description

derived *group*	Keyword to display information about the cached PPPoE configuration for the specified PPPoE group.
relay	Keyword to display PPPoE relay information.
context all	Keyword to display PPPoE information about all relay contexts.
session	Keyword to display summary information about PPPoE neighbor sessions.
all	Keyword to display detailed information on all PPPoE neighbor sessions.
interface	Displays detailed neighbor session information for the specified interface.
packets	Keyword to display PPPoE neighbor session packet statistics.
summary	Keyword to display summary information about PPPoE neighbor sessions.
throttled mac	Keyword to display information about PPPoE MAC addresses that are throttled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and was enhanced to display information about relayed PPPoE Active Discovery (PAD) messages.

Examples

The following example shows output for the **show pppoe session** command:

```
Router# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total

Uniq ID PPPoE RemMAC Port Source VA State
SID LocMAC VA-st
Uniq ID       PPPoE SID   RemMAC          Port    VT    VA    State    LocMAC    VA-st
N/A             10        aabb.cc01.5830   Et0/3  Vt1  Vi3    PTA    aabb.cc01.5930 UP
```

Table A-11 describes the significant fields shown in the display.

Table A-11 show pppoe sessions Field Descriptions

Field	Description
Uniq ID	The unique identifier for the PPPoE neighbor session.
PPPoE SID	The PPPoE neighbor session identifier.
RemMAC Local MAC	The MAC address for remote end point of the PPPoE neighbor session and the MAC address for the router interface of the PPPoE neighbor session.
Port	The interface on the router in the PPPoE neighbor session.
VT	The virtual terminal in the PPPoE neighbor session.
VA VA-st	The virtual access and virtual access state for the PPPoE neighbor session.
State	The state of the PPPoE neighbor session.

show pppoe derived

To display the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile, use the **show pppoe derived** command in privileged EXEC mode.

show pppoe derived group *group-name*

Syntax Description

group *group-name*	PPPoE profile for which the cached PPPoE configuration displays.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

A subscriber profile can be configured locally on the router or remotely on a AAA server. The PPPoE configuration that is derived from a subscriber profile is cached locally under the PPPoE profile. Use the **show pppoe derived** command to display the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile.

A subscriber profile contains a list of PPPoE service names. The PPPoE server will advertise the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile. A subscriber profile is assigned to a PPPoE profile by using the **service profile** command in BBA group configuration mode.

Examples

The following example shows the PPPoE configuration for PPPoE profile that is derived from subscriber profile. The services are advertised to each PPPoE client connection that uses PPPoE profile.

```
Router# show pppoe derived group subscriber_1
Derived configuration from subscriber profile 'subscriber_1':
Service names:
manet_radio
```

Related Commands

Command	Description
clear pppoe derived	Clears the cached PPPoE configuration of a PPPoE profile and forces the PPPoE profile to reread the configuration from the assigned subscriber profile.
pppoe service	Adds a PPPoE service name to a local subscriber profile.
service profile	Assigns a subscriber profile to a PPPoE profile.
subscriber profile	Defines Subscriber Service Switch policy for searches of a subscriber profile database.

show pppoe session

To display information about currently active PPPoE neighbor sessions, use the **show pppoe session** command in privileged EXEC mode.

show pppoe session [**all** | **packets**]

Syntax Description

all	(Optional) Keyword to display detailed information about the PPPoE neighbor session.
packets	(Optional) Keyword to display packet statistics for the PPPoE neighbor session.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)YG	This command was introduced on the Cisco SOHO 76, 77, and 77H routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and was enhanced to display information about relayed PPPoE Active Discovery (PAD) messages.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and support was added for the Cisco 7200, 7301, 7600, and 10000 series platforms.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and the output following the use of the **all** keyword was modified to indicate if a neighbor session is Interworking Functionality (IWF)-specific or if the **tag ppp-max-payload** tag is in the discovery frame and accepted.
12.4(15)XF	The output was modified to display VMI and PPPoE process-level values.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support VMIs in MANETs.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Examples

Single Neighbor Session: Example

The following is example output from the **show pppoe session** command:

```
Router# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total

Uniq ID PPPoE RemMAC Port Source VA State
SID LocMAC VA-st
Uniq ID       PPPoE SID   RemMAC          Port    VT    VA    State    LocMAC     VA-st
N/A             10        aabb.cc01.5830   Et0/3  Vt1   Vi3     PTA    aabb.cc01.5930 UP
```

Table A-12 describes the significant fields shown in the displays.

Table A-12 show pppoe session Field Descriptions

Field	Description
Uniq ID	Unique identifier for the PPPoE neighbor session.
PPPoE SID	PPPoE neighbor session identifier.
RemMAC	Remote MAC address.
Port	Port type and number.
VT	Virtual-template interface.
VA	Virtual access interface.
State	Displays the state of the neighbor session, which will be one of the following: • FORWARDED • FORWARDING • LCP_NEGOTIATION • LOCALLY_TERMINATED • PPP_START • PTA • RELFWD (a PPPoE neighbor session was forwarded for which the Active discovery messages were relayed) • SHUTTING_DOWN • VACCESS_REQUESTED
LocMAC	Local MAC address.

Related Commands

Command	Description
clear pppoe relay context	Clears PPPoE relay contexts created for relaying PAD messages.
show pppoe relay context all	Displays PPPoE relay contexts created for relaying PAD messages.

show r2cp clients

To display R2CP clients, use the **show r2cp clients** command in privileged EXEC mode.

show r2cp clients

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

Use the **show r2cp clients** command to exchange metric information with the radio—either for all radio clients on all interfaces or for one radio client on a specific interface.

Examples

Show all radio clients on all interfaces example

The following example shows how to display all radio clients on all interfaces:

```
Router# show r2cp clients
R2CP Clients for all interfaces:

R2CP Clients for Interface FastEthernet0/1
R2CP Server IP=12.12.12.101:28672 Sock=1

R2CP Client ID=1 IP=12.12.12.7:5500
 node heartbeat missed count=0
 node heartbeat interval=5 seconds
 node heartbeat missed threshold=3
 node terminate ack missed count=0
 node terminate ack timeout=1000 milliseconds
 node terminate ack missed threshold=3
 session activity timeout=1 minutes
 session terminate ack timeout=1000 milliseconds
 session terminate ack missed threshold=3
No Virtual Template defined.
```

Show all radio clients on all interfaces example

The following example shows how to display one radio client on a specific interface:

```
Router# show r2cp fastethernet 0/1
r2cp clients fastEthernet 0/1

R2CP Clients for Interface FastEthernet0/1
R2CP Server IP=12.12.12.101:28672 Sock=1

R2CP Client ID=1 IP=12.12.12.7:5500
 node heartbeat missed count=0
 node heartbeat interval=5 seconds
 node heartbeat missed threshold=3
 node terminate ack missed count=0
 node terminate ack timeout=1000 milliseconds
 node terminate ack missed threshold=3
 session activity timeout=1 minutes
 session terminate ack timeout=1000 milliseconds
 session terminate ack missed threshold=3
 No Virtual Template defined.
```

Related Commands

Command	Description
show r2cp config	Displays router configuration information details for the R2CP interface.
show r2cp neighbors	Displays neighbors on an R2CP interface indicating radio capabilities from a Layer 3, next-hop perspective.

show r2cp config

To display R2CP configuration, use the **show r2cp config** command in privileged EXEC mode.

show r2cp config

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

Use the **show r2cp config** command to display router configuration details for the R2CP interface. These details include the following components:

- Heartbeat threshold
- Node-terminate acknowledgement threshold
- Node-terminate acknowledgement timeout
- Port number
- Session-activity timeout
- Session-terminate acknowledgement threshold
- Session-terminate acknowledgement timeout
- Virtual access template number

Examples

Display R2CP router configuration details example

The following example shows how to display configuration details for the R2CP interface:

```
Router# show r2cp config
R2CP Configuration from FastEthernet0/1

R2CP Server IP=12.12.12.101:28672
 node heartbeat missed threshold=3
 node terminate ack timeout=2200 milliseconds
 node terminate ack missed threshold=2
 session activity timeout=3 minutes
 session terminate ack timeout=1000 milliseconds
 session terminate ack missed threshold=5
 virtual template=220
```

Related Commands

Command	Description
show r2cp clients	Displays radio client information for one or more clients on the R2CP interface.
show r2cp neighbors	Displays neighbors on an R2CP interface radio capabilities from a Layer 3, next-hop perspective.

show r2cp neighbors

To show neighbors for R2CP, including two radio neighbor sessions, use the **show r2cp neighbors** command in privileged EXEC mode.

show r2cp neighbors

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2) GC	This command was introduced.

Usage Guidelines

The Cisco 5930 ESR does not support this comand.

View neighbors on an R2CP interface to display information about the neighbor with which the radio can talk from a Layer 3, next-hop perspective. The **show r2cp neighbors** command output allows you to get metric data associated with a next-hop, so you can better understand the paths that the traffic is taking.

Examples

The following example shows metric data for R2CP neighbor sessions:

```
Router# show r2cp neighbors

R2CP Neighbors for all interfaces:

R2CP Neighbors for Interface FastEthernet0/1
R2CP Server IP=12.12.12.101:28672 Sock=1

  Global Session ID=101
 MAC Address: 1122.3344.5566
 Vlan ID: 0
 Metrics:  rlq=100  resources=100  latency=10 milliseconds
           cdr=100000 Kbps  mdr=100000 Kbps
```

Related Commands

Command	Description
show r2cp clients	Displays metric data for R2CP neighbor sessions.
show r2cp config	Displays detailed R2CP configuration.

show vmi counters

The **show vmi counters** command in privileged EXEC mode displays input and output counts.

show vmi counters [*vmi-interface*]

Syntax Description

vmi-interface	(Optional) Number assigned to the VMI interface.

Command Default

If no VMI interface is specified, counters for all VMI interfaces are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Examples

The following example shows how to display the VMI input and output counts for DLEP:

```
Router# show vmi counters vmi1

1 vmi counters

Input Counts:
  Process Enqueue      =        37 (PHY)          18/1 (VMI)
  Fastswitch           =      1005
  BMA Fast Path Drop   =         0
  BMA Punt Drop:
       Total           =         0
       Dot1q Error     =         0
       Queue Full      =         0
       Not Permitted   =         0
  VMI Punt Drop:
       Queue Full      =         0
  BMA Mac Match        =         8 (mcast)       1016 (ucast)
  BMA Mac NoMatch      =        35 (Fast)          35 (Punt)

Output Counts:
  Transmit:
       VMI Process DQ  =        31
       Fastswitch VA   =      1005
       Fastswitch VMI  =         0
  Drops:
       Total           =        14
       QOS Error       =         0
       Encap Error     =         0
       Transport Error =         0
       Interface Error =         0
       L2 Send Error   =         0
       Mcast NBR Error =         0
       Ucast NBR Error =        14
DPD_2951_1#
```

```
Router#
```

The following example shows vmi counts for PPPoE.

```
Router#show vmi counters vmi 2

Input Counts:
  Process Enqueue      =         10(VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =          2
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Router#
```

The following example shows vmi counts for DLEP.

```
Router# show vmi counters vmi 2

Input Counts:
  Process Enqueue      =         10 (PHY)            1/0 (VMI)
  Fastswitch           =          0
  BMA Fast Path Drop   =          0
  BMA Punt Drop:
       Total           =          0
       Dot1q Error     =          0
       Queue Full      =          0
       Not Permitted   =          0
  VMI Punt Drop:
       Queue Full      =          0
  BMA Mac Match        =          1 (mcast)          0 (ucast)
  BMA Mac NoMatch      =          9 (Fast)           9 (Punt)

Output Counts:
  Transmit:
       VMI Process DQ  =          2
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       Encap Error     =          0
       Transport Error =          0
       Interface Error =          0
       L2 Send Error   =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Router#
```

Table A-14 describes the count definitions in the **show vmi counters** command display.

Table A-13 show vmi counters Count Definitions

Count	Definition
Input Counts:	
Process Enqueue	Number of packets enqueued to the Physical or VMI input queue.
Fastswitch	Number of packets fastswitched.
BMA Fast Path Drop	Number of Broadcast Multi-Access (BMA) packets dropped in the fast path due to resource issues.
BMA Punt Drop Total	Total number of BMA drops
BMA Punt Drop – Dot1q Error	Number of BMA packets that are unable to match the 802.1q tag.
BMA Punt Drop – Queue Full	Number of BMA VMI input queue full during BMA punt.
BMA Punt Drop – Not Permitted	Number of BMA Unicast and Multicast packets NOT permitted on this interface.
VMI Punt Drop – Queue Full	Number of BMA VMI input queues full during Non-BMA punt.
BMA Mac Match	Number of Unicast and Multicast packets that match the VMI neighbor.
BMA Mac NoMatch	Number of BMA Unicast and Multicast packets that do not match a VMI neighbor.
Output Counts:	
Transmit – VMI Process DQ	Number of packets dequeued from the VMI output queue.
Transmit – Fastswitch VA	Number of packets fastswitched out the VA interface.
Transmit – Fastswitch VMI	Number of packets fastswitched out the VMI Interface.
Drops – Total	Total number of packets dropped.
Drops – QOS Error	Number of packets dropped due to QoS error.
Drops – Encap Error	Number of packets dropped when unable to create an encap.
Drops – Transport Error	Number of packets dropped due to transport mismatch.
Drops – Interface Error	Number of packets dropped due to interface mismatch.
Drops – L2 Send Error	Number of packets dropped due to L2 resource error.
Drops – Mcast NBR Error	Number of packets dropped due to multicast neighbor not found.
Drops – Ucast NBR Error	Number of packets dropped due to unicast neighbor not found.

show vmi neighbors

To display information about neighbor connections to the VMI, use the **show vmi neighbors** command in privileged EXEC mode.

show vmi neighbors [**detail**] [*vmi-interface*]

Syntax Description

detail	(Optional) Keyword to display details about the VMI neighbors.
vmi-interface	(Optional) Number of the VMI interface.

Command Default

If no arguments are specified, information about all neighbors for all VMI interfaces displays.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.3(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The **show vmi neighbors** command provides a list of devices that have been dynamically discovered by the connected radio devices in a router-to-radio network, and for which connectivity has been achieved through PPPoE and the radio network.

Examples

The following is example output from the **show vmi neighbors** command used to display dynamically created neighbors on a VMI interface:

```
Router# show vmi neighbors vmi1

1 vmi1 Neighbors

           IPV6       IPV4                         Transmit    Receive
Interface  Address    Address       Uptime       Packets     Packets
vmi1       ::         10.3.3.2      00:02:11     0000000008  0000000073
Router#
```

Table A-14 describes the significant fields shown in the **show vmi neighbors** command display.

Table A-14 show vmi neighbors Field Descriptions

Field	Description
Interface	The interface number.
IPv6 Address	IPv6 address of the neighbor.
IPv4 Address	IPv4 address of the neighbor.

Table A-14 show vmi neighbors Field Descriptions (continued)

Field	Description
Uptime	How long the interface has been up. Time shown in hh:mm:ss format.
Transmit Packets	Number of packets transmitted from the interface during the monitored up time.
Received Packets	Number of packets received on the interface during the monitored up time.

show vmi neighbors command with detail keyword: Example

The following example shows the details about the known VMI neighbors:

```
Router# show vmi neighbors detail

              1 vmi1 Neighbors


vmi1   IPV6 Address=::
       IPV4 Address=10.20.1.6, Uptime=00:00:23
       Output pkts=0, Input pkts=3
       No Session Metrics have been received for this neighbor.
       Transport PPPoE, Session ID=2
       INTERFACE STATS:
          VMI Interface=vmi1,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access3,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=FastEthernet0/0,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
    Local Credits: 65524   Peer Credits: 65524   Scalar Value 64 bytes
    Credit Grant Threshold: 28000    Max Credits per grant: 65534
    Credit Starved Packets: 0
    PADG Seq Num: 24     PADG Timer index: 0
    PADG last rcvd Seq Num: 24
    PADG last nonzero Seq Num: 0
    PADG last nonzero rcvd amount: 0
    PADG Timers: [0]-1000    [1]-2000    [2]-3000    [3]-4000
    PADG xmit: 24  rcvd: 24
    PADC xmit: 24  rcvd: 24
    PADQ xmit: 0  rcvd: 0
Router#
```

Table A-15 describes the significant fields shown in the **show vmi neighbors detail** command display.

Table A-15 show vmi neighbors detail Field Descriptions

Field	Description
Interface	The interface number.
IPv6 Address	IPv6 address of the neighbor.
IPv4 Address	IPv4 address of the neighbor.
Uptime	How long the interface has been up. Time shown in hh:mm:ss format.
Output pkts	Number of outgoing packets during the recorded up time.
Input pkts	Number of incoming packets during the recorded up time.

Table A-15 show vmi neighbors detail Field Descriptions (continued)

Field	Description
Metric Data	The Metric data statistics **Total rcvd**: The total number of packets received on the interface. **Avg arrival rate**: The average arrival rate for each packet in milliseconds. **CURRENT**: The current values for the following statistics: Metric Data Rate (MDR), Credit Data Rate (CDR), Latency (Lat), Resource (Res), Root Link Query (RLQ), and the load. **MDR**: The maximum, minimum, and average metric data rate. **CDR**: The maximum, minimum, and average credit data rate. **Latency**: The maximum, minimum, and average latency. **Resource**: The maximum, minimum, and average resource. **RQL**: The maximum, minimum, and average RQL. **Load**: The maximum, minimum, and average load.
Transport	The routing protocol, in this case–PPPoE.
Session ID	The identifier of the VMI session.
INTERFACE STATS	A series of statistics collected on the interface and shows for each of the VMI interface, virtual access interface, and the physical interface. For each interface, statistics display indicating the number of packets in the input and output queues and the number of packets dropped from each queue.
PPPoE Flow Control Stats	The statistics collected for PPPoE credit flow. **Local Credits**: The number of credits belonging to this node. **Peer Credits**: The number of credits belonging to the peer. **Scalar Value**: The credit grant in bytes specified by the radio. **Credit Grant Threshold**: The number of credits below which the peer needs to dip before this node sends an inband or out-of-band grant. **Credit Starved Packets**: The number of packets dropped or queued due to insufficient credits from the peer. **Max Credits per grant**: 65534. **PADG Seq Num**: The sequence number for the PPPoE packet discovery grant. **PADG Timer index**: The timer index for the PPPoE packet discovery grant. **PADG last rcvd Seq Num**: The sequence number for the previously received PPPoE packet discovery grant. **PADG last nonzero Seq Num**: The sequence number for the last non-zero PPPoE packet discovery grant. **PADG last nonzero rcvd amount**: The received amount in the last non-zero PPPoE packet discovery grant. **PADG Timers**: The PPPoE packet discovery grant timers. **PADG xmit**: *numberic* **rcvd**: The number of PPPoE packet discovery grants transmitted and received. **PADC xmit**: **133 rcvd: 133:** The number of PPPoE packet discovery grant confirmations transmitted and received. **PADQ xmit**: **0 rcvd**: The number of PPPoE packet discovery quality grants transmitted and received.

Related Commands

Command	Description
debug vmi	Displays debugging output for VMIs.
interface vmi	Creates a virtual multipoint interface (VMI) that can be configured and applied dynamically.

shutdown

To deactivate an IP multiplexing profile, enter the **shutdown** command. To activate an IP multiplexing profile, use the **no** form of the command.

shutdown

[**no**] **shutdown**

Command Modes

IP multiplexing configuration (config-ipmux-profile)

IPv6 multiplexing configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

You must enter the **no shutdown** command to activate an IP multiplexing profile so that the IP multiplexing packet handler processes packets for IP multiplexing. A disabled multiplexing profile cannot send superframes, but will accept incoming superframes which match its configured source and destination addresses.

If you want to change the ACL associated with the profile, or edit the ACL associated with the profile, you must enter the **shutdown** command. After you have changed either the access-list or the ACL associated with the profile, you then enter the **no shutdown** command to clear the IP multiplexing cache and use the new information.

A multiplexing profile must have both a source and destination address configured in order to be activated.

Examples

The following example shows how to activate the IP multiplexing profile *routeRTP-SJ*.

```
router#configure terminal
router(config)#ipv6 mux profile routeRTP-SJ
router(config-ipmux-v6)#no shutdown
router(config-ipmux-v6)#exit
router(config)#
```

singlepacket

Interesting data packets are always transmitted inside a superframe, even if there is only one packet to transmit when the hold timer expires. If you want the IP multiplexing packet handler not to create single packet superframes, enter the **no singlepacket** command. If you want to send single packet superframes, enter the singlepacket command.

singlepacket

[**no**] **singlepacket**

Command Modes

IP multiplexing configuration (config-ipmux-profile)

IPv6 multiplexing configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

By default the IP multiplexing packet handler creates single packet superframes.

Single packet multiplexing applies to all hold queues for a given IP multiplexing profile.

Examples

The following example shows how to configure single packet superframes for IP multiplexing profile *routeRTP-SJ*.

```
router#configure terminal
router(config)#ipv6 mux profile routeRTP-SJ
router(config-ipmux-v6)#singlepacket
router(config-ipmux-v6)#exit
router(config)#
```

source

To specify the IPv4 or IPv6 source address for the local endpoint of the IP multiplexing path, enter the **source** command. To clear the source address, use the **no** form of the command.

source {*ip_addr* | *ipv6_addr* | **interface** *interface_type*}

[**no**] **source**

Syntax Description

ip_addr	IPv4 address for the source local endpoint of the IP multiplexing path.
ipv6_addr	IPv6 address for the source local endpoint of the IP multiplexing path.
interface *interface_type*	Physical interface for the source local endpoint of the IP multiplexing path.

Command Modes

IP multiplexing configuration (config-ipmux-profile)

IPv6 multiplexing configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

You must configure a source address for the profile in order to use it. If you attempt to issue a no shutdown command when no source address is configured, you will be prompted to configure a source address. If a profile is active, you must issue a shutdown command before changing the source address.

If you enter the **source** command again, then the new address overwrites the previously entered address.

An incoming superframe must match its source and destination addresses to the destination and source addresses, respectively, in the multiplexing profile in order for the superframe to be demultiplexed. If either address does not match, the superframe is ignored.

Examples

The following example shows how to configure the IPv6 address *FE80::A8BB:CCFF:FE01:5700* as the source address for superframe packets.

```
router#configure terminal
router(config)#ipv6 mux profile routeRTP-SJ
router(config-ipmux-v6)#source FE80::A8BB:CCFF:FE01:5700
router(config-ipmux-v6)#exit
router(config)#
```

summary-prefix (OSPFv3)

To configure an IPv6 summary prefix, use the **summary-prefix** command in router address-family configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

no summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

Syntax Description

prefix	IPv6 route prefix for the destination.
not-advertise	(Optional) Suppress routes that match the specified prefix and mask pair. This keyword applies to OSPF only.
tag *tag-value*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps. This keyword applies to OSPF only.

Command Default

No IPv6 summary prefix is defined.

Command Modes

Router address family configuration (config-rtr-af)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **summary-prefix** command can be used to summarize routers redistributed from other routing protocols. Multiple groups of addresses 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.

Examples

In the following example, the summary prefix FEC0::/24 includes addresses FEC0::/1 through FEC0::/24. Only the address FEC0::/24 is advertised in an external LSA.

```
Router(config)# router ospfv3 100
Router(config-rtr)# router-id 4.4.4.4
Router(config-rtr)# address-family ipv4 unicast
Router(config-rtr-af)summary-prefix FEC0::/24
Router(config-rtr-af)#exit
```

```
Router# show ospfv3 summary-prefix
OSPFv3 Process 100, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
OSPFv3 Process 200, Summary-prefix
Not configured
```

timers manet

To configure MANET timer parameters, use the **timers manet** command in router-configuration mode. To restore the timer default values, use the **no** form of this command.

timers manet {**ackwait** *ackwait-value* | **peering** *peering-value* | **pushback** *pushback-value*}

no timers manet {**ackwait** *ackwait-value* | **peering** *peering-value* | **pushback** *pushback-value*}

Syntax Description

ackwait	Keyword for Acknowledgment wait timer.
ackwait-value	Value specified in milliseconds. The default value is 1000 milliseconds. Valid values range from 0 to 10,000.
peering	Keyword used to specify the redundant peering delay timer value.
peering-value	Value specified in milliseconds. The default is 250 milliseconds. Valid values range from 0 to 10,000.
pushback	Keyword for MANET pushback timer set to assist in regulating traffic when flooding occurs because multiple non-primary relays flood at the same time.
pushback-value	Value specified in milliseconds. The default is 2000 milliseconds. Valid values range is from 0 to 60,000 milliseconds.

Command Modes

Router configuration (config-rtr)

Command History

Release	Modification
12.4(24) GC	This command was introduced.

Usage Guidelines

Timers on MANET Interfaces

Non-active relays do not immediately start helping with flooding. Timers can be configured to delay Non-active relays until the active relay finishes its procedure. The **timers manet** command is used to configure these timers.

Peering Timers on MANET Interfaces

When selective peering is enabled, this timer determines how long the OSPFv3 process waits between selective peering decisions. Use the **peering** keyword to specify how long the router waits between selective peering decisions.

Acknowledgements on MANET Interfaces

When sending acknowledgments on a MANET interface, a small delay is configured in order to accumulate as many acknowledgments as possible into a single ACK message to reduce the number of messages being sent. Use the **ackwait** *ackwait-value* keyword and argument to set the acknowledgment wait timer.

Pushback Timers on MANET Interfaces

Use the **pushback** keyword to help prevent multiple non-primary relays from flooding at the same time. If a relay has already seen all of the acknowledgements from the nodes for which it is going to relay, it will cancel the pushback timer.

The default value for the pushback timer is 50 percent of the retransmit timer value.

Examples

The following example shows how to set the MANET pushback timer to 50,000 milliseconds, the MANET acknowledgement timer to 1001 milliseconds, and the MANET peering timer to 1000 seconds:

```
Router(config)#router ospfv3 100
Router(config-router)#router-id 1.1.1.1
Router(config-router)#address-family ipv6 unicast
Router(config-router-af)#exit
Router(config-router)#timers manet pushback 50000
Router(config-router)#timers manet ackwait 1001
Router(config-router)#timers manet peering 1000
Router(config-router)#end

Router#show running-config | be router ospfv3 100
router ospfv3 100
 router-id 1.1.1.1
 timers manet ackwait 1001
 timers manet pushback 50000
 timers manet peering 1000
 !
 address-family ipv6 unicast
 exit-address-family
!
Router#
```

Related Commands

Command	Description
manet cache	Configures the number of MANET cached LSA, updates and acknowledgments.
manet selective peering	Enables selective peering on a per-area or per-interface basis and configures the maximum number of redundant paths to each neighbor.

timers throttle spf

To turn on Open Shortest Path First (OSPF) for IPv6 shortest path first (SPF) throttling, use the **timers throttle spf** command in router-configuration mode. To turn off SPF throttling, use the **no** form of this command.

timers throttle spf *delay next-delay holdtime*

no timers throttle spf

Syntax Description

delay	Initial delay before the spf calculation in milliseconds. The default is 10 seconds. Valid values range from 0 to 60,000 milliseconds.
next-delay	Delay in milliseconds between the first and second spf calculations receiving a change in the SPF calculation. The default is 5000 milliseconds (5 seconds). Valid values range from 0 to 600000 milliseconds.
nextdelay holdtime	Hold time (in seconds) between consecutive SPF calculations. The default is 10 seconds. Valid values range from 0 to 600000.

Command Default

OSPF for IPv6 throttling is always enabled.

Command Modes

Router configuration (config-rtr)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(24)GC	This command was integrated into Cisco IOS Release 12.4(24)GC.

Usage Guidelines

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *delay* argument.

Use the *next-delay* argument to set the delay between the first and second SPF calculations.

Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *holdtime* argument. Subsequent wait times remain at the maximum until the values are reset or an LSA is received between SPF calculations.

When you configure an OSPFv3 network manet for any interface attached to the OSPFv3 process, the default values for the delay, next-delay, and hold time are reduced to 1000 milliseconds, 1000 milliseconds, and 2000 milliseconds respectively.

Examples

The following example shows a router with the *delay* and *next-delay* interval values configured at 40 milliseconds, and the holdtime value to 50 milliseconds**:**

```
Router(config)# router ospfv3 1
Router(config-router)# timers throttle spf 40 40 50
Router(config-router)#exit
Router#
```

Related Commands

Command	Description
show ospfv3	Displays general information about OSPF for IPv6 routing processes.

ttl

To insert into the superframe header the time-to-live (TTL) value for outbound superframes, enter the **ttl** command. To reset the TTL to 64 hops, use the **no** form of this command.

ttl *hops*

[**no**] **ttl**

Syntax Description

hops	Number of hops equivalent to the TTL value inserted into the IP header of the outbound superframe. Valid values range from 1 to 255 hops.

Command Modes

IP multiplexing configuration (config-ipmux-profile)

IPv6 multiplexing configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.

Usage Guidelines

If you do not specify an TTL, the IP multiplex packet handler uses the default value of 64 hops.

If you enter the **ttl** command again, then the new TTL value overwrites the previously entered size.

Examples

The following example shows how to configure the TTL size for IP multiplexing profile *routeRTP-SJ* to *255 hops*.

```
router#configure terminal
router(config)#ipv6 mux profile routeRTP-SJ
router(config-ipmux-v6)#ttl 255
router(config-ipmux-v6)#exit
router(config)#
```

APPENDIX B

System Message Overview

This publication lists and describes the Cisco IOS system error messages specific to Cisco IOS Release 15.2(4)GC. The system software sends these error messages to the console (and, optionally, to a logging server on another system) during operation. Not all system error messages indicate problems with your system. Some messages are purely informational, while others may help diagnose problems with communications lines, internal hardware, or the system software.

This publication also includes error messages that appear when the system fails.

This chapter contains the following sections:

- System Message Structure, page B-1
- System Message Example, page B-2
- Using the Error Message Decoder to Search for System Messages, page B-3
- Error Message Traceback Reports, page B-3
- Error Messages, page B-3

System Message Structure

System error messages are structured as follows:

FACILITY-SEVERITY-MNEMONIC: Message-text

- FACILITY code

  The facility code consists of two or more uppercase letters that indicate the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software. Table B-1 lists the system facility codes.

Table B-1 Facility Codes

Code	Facility
IPMUX	IP Mutiplexing

- SEVERITY level

  The severity level is a single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation. Table B-2 lists the message severity levels.

Table B-2 Message Severity Levels

Severity Level	Description
0 – emergency	System is unusable
1 – alert	Immediate action required
2 – critical	Critical condition
3 – error	Error condition
4 – warning	Warning condition
5 – notification	Normal but significant condition
6 – informational	Informational message only
7 – debugging	Message that appears during debugging only

- MNEMONIC code

  The MNEMONIC code uniquely identifies the error message.

- Message-text

  Message-text is a text string that describes the condition. The text string sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because variable fields change from message to message, they are represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec]. Table B-3 lists the variable fields in messages.

Table B-3 Representation of Variable Fields in Messages

Representation	Type of Information
[chars] or [char]	Character string
[dec]	Decimal
[hex]	Hexadecimal integer
[int]	Integer
[num]	Number

System Message Example

The following is an example of a system error message:

LINK-2-BADVCALL: Interface [chars], undefined entry point

- LINK is the facility code.
- 2 is the severity level.
- BADVCALL is the mnemonic code.
- “Interface [chars], undefined entry point” is the message text.

Using the Error Message Decoder to Search for System Messages

The Error Message Decoder (EMD) is a tool that will help you to research and resolve error messages for Cisco software. EMD helps you to understand the meaning of the error messages that display on the console of Cisco routers, switches, and firewalls.

To use the EMD, copy the message that appears on the console or in the system log, paste it into the window, and press the Submit button. You will automatically receive an Explanation, Recommended Action, and, if available, any related documentation for that message.

The EMD is located here:

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

Searching for System Messages in Online Documentation

search for messages in online documentation, use the search function of your browser by copying and pasting the message that appears on the console or in the system log.

Some messages that appear on the console or in the system log indicate where the system condition occurred. These messages are structured as follows:

FACILITY-SOURCE-SEVERITY-MNEMONIC: Message-text

SOURCE indicates the location of the condition. Examples of SOURCE are SP, which indicates that the condition occurred in the switch processor, or DFC5, which indicates that the condition occurred in the Distributed Forwarding Card on the module in slot 5.

If you search for the explanation and recommended action of a message that contains a SOURCE, remove the SOURCE from the text first, and then search for the message in the documentation.

For example, instead of searching the documentation for the message C6KPWR-SP-4-DISABLED, remove the SOURCE identifier and search for the message C6KPWR-4-DISABLED.

Error Message Traceback Reports

Some messages describe internal errors and contain traceback information. This information is very important and should be included when you report a problem to your technical support representative.

The following sample message includes traceback information:

-Process = "Exec", level = 0, pid = 17

-Traceback = 1A82 1AB4 6378 A072 1054 1860

Error Messages

This section lists the switch system messages by facility. Within each facility, the messages are listed by severity levels 0 to 7. The highest severity level is 0, and the lowest severity level is 7. Each message is followed by an explanation and a recommended action.

Note The messages listed in this chapter do not include the date/time stamp designation; the date/time stamp designation is displayed only if the software is configured for system log messaging.

IPMUX

This section contains theIP Mutliplexing (IPMUX) messages.

IPMUX-3

Error Message `IPMUX-3-V4_CACHE_FULL: IPMux V4 Cache full - replacing active entry`

Explanation This message indicates that the IPv4 multiplexing cache is full and each subsquent entry to the cache deletes a current IPv4 multiplexing cache entry.

Recommended Action Increase the IPv4 multiplexing cache using the **ip mux cache** command.

Error Message `IPMUX-3-V6_CACHE_FULL: IPMux V6 Cache full - replacing active entry`

Explanation This message indicates that the IPv6 multiplexing cache is full and each subsquent entry to the cache deletes a current IPv6 multiplexing cache entry.

Recommended Action Increase the IPv6 multiplexing cache using the **ipv6 mux cache** command.

APPENDIX C

Technical Support Reference

This appendix provides the following major sections strictly for reference while working with Cisco Technical Support:

- Default Settings for DLEP, page C-1

Default Settings for DLEP

This section provides the following procedure as an example of how to change DLEP configuration settings:

- Configuring the Heartbeat Threshold, page C-2

Caution Do not change the default DLEP configuration unless a Cisco Support engineer instructs you to do so. The procedure in this section is available only for reference while working with Cisco Technical Support.

If directed to do so, see Appendix A, “Command Reference”pages:

Configuring the Heartbeat Threshold

The heartbeat threshold indicates the maximum number of consecutively missed heartbeats allowed on the DLEP interface before declaring a failed association.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface*
4. **ip dlep set heartbeat-threshold** *count*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode.

Step 3	`interface` *`interface`*
	Example:
	`Router# interface fa0/1`
	`Router(config-if)#`
		Specifies the interface and places the router in interface-configuration mode.

Step 4	`ip dlep set heartbeat-threshold` *`count`*
	Example:
	`Router(config-if)# ip dlep set heartbeat-threshold 3`
		Sets the heartbeat threshold. The heartbeat-threshold valid range is from 2 to 8.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits the current mode.