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)#
```