IPv6 Commands: ipv6 su to m

ipv6 summary-address eigrp

To configure a summary aggregate address for a specified interface, use the **ipv6**summary-address **eigrp**command in interface configuration mode. To disable a configuration, use the **no** form of this command.

ipv6 summary-address eigrp *as-number ipv6-address* [*admin-distance*]

no ipv6 summary-address eigrp *as-number ipv6-address* [*admin-distance*]

Syntax Description

as-number	Autonomous system number.
ipv6-address	Summary IPv6 address to apply to an interface.
admin-distance	(Optional) Administrative distance. A value from 0 through 255. The default value is 90.

Command Default

An administrative distance of 5 is applied to Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 summary routes. EIGRP for IPv6 automatically summarizes to the network level, even for a single host route. No summary addresses are predefined.

Command Modes

Interface configuration

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

The **ipv6 summary-address eigrp** command is used to configure interface-level address summarization. EIGRP for IPv6 summary routes are given an administrative distance value of 5. The administrative distance metric is used to advertise a summary address without installing it in the routing table.

Examples

The following example provides a summary aggregate address for EIGRP for IPv6 for AS 1:

```
ipv6 summary-address eigrp 1 2001:0DB8:0:1::/64
```

ipv6 tacacs source-interface

To specify an interface to use for the source address in TACACS packets, use the **ipv6 tacacs source-interface**command in global configuration mode. To remove the specified interface from the configuration, use the **no** form of this command.

ipv6 tacacs source-interface *interface*

no ipv6 tacacs source-interface *interface*

Syntax Description

interface	Interface to be used for the source address in TACACS packets.

Command Default

No interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **ipv6 tacacs source-interface**command specifies an interface to use for the source address in TACACS packets.

Examples

The following example shows how to configure the Gigabit Ethernet interface to be used as the source address in TACACS packets:

```
Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

ipv6 traffic interface-statistics

To collect IPv6 forwarding statistics for all interfaces, use the **ipv6 traffic interface-statistics**command in global configuration mode. To ensure that IPv6 forwarding statistics are not collected for any interface, use the **no** form of this command.

ipv6 traffic interface-statistics [unclearable]

no ipv6 traffic interface-statistics [unclearable]

Syntax Description

unclearable	(Optional) IPv6 forwarding statistics are kept for all interfaces, but it is not possible to clear the statistics on any interface.

Command Default

IPv6 forwarding statistics are collected for all interfaces.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Using the optional unclearable keyword halves the per-interface statistics storage requirements.

Examples

The following example does not allow statistics to be cleared on any interface:

```
ipv6 traffic interface-statistics unclearable
```

ipv6 traffic-filter

To filter incoming or outgoing IPv6 traffic on an interface, use the **ipv6 traffic-filter**command in interface configuration mode. To disable the filtering of IPv6 traffic on an interface, use the **no** form of this command.

ipv6 traffic-filter *access-list-name* {**in**| **out**}

no ipv6 traffic-filter *access-list-name*

Syntax Description

access-list-name	Specifies an IPv6 access name.
in	Specifies incoming IPv6 traffic.
out	Specifies outgoing IPv6 traffic.

Command Default

Filtering of IPv6 traffic on an interface is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.2(33)SXI4	The **out** keyword and therefore filtering of outgoing traffic is not supported in IPv6 port-based access list (PACL) configuration.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.

Release	Modification
12.2(50)SY	This command was modified. The **out** keyword is not supported.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Examples

The following example filters inbound IPv6 traffic on Ethernet interface 0/0 as defined by the access list named cisco:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 traffic-filter cisco in
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 unicast-routing

To enable the forwarding of IPv6 unicast datagrams, use the **ipv6 unicast-routing**command in global configuration mode. To disable the forwarding of IPv6 unicast datagrams, use the **no** form of this command.

ipv6 unicast-routing

no ipv6 unicast-routing

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 unicast routing is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series devices.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Usage Guidelines

Configuring the **no ipv6 unicast-routing** command removes all IPv6 routing protocol entries from the IPv6 routing table.

Examples

The following example enables the forwarding of IPv6 unicast datagrams:

```
Device(config)# ipv6 unicast-routing
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 enable	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 route	Displays the current contents of the IPv6 routing table.

ipv6 unnumbered

To enable IPv6 processing on an interface without assigning an explicit IPv6 address to the interface, use the **ipv6 unnumbered**command in interface configuration mode. To disable IPv6 on an unnumbered interface, use the **no** form of this command.

ipv6 unnumbered *interface-type* **interface-number**

no ipv6 unnumbered

Syntax Description

interface-type	The interface type of the source address that the unnumbered interface uses in the IPv6 packets that it originates. The source address cannot be another unnumbered interface.
interface-number	The interface number of the source address that the unnumbered interface uses in the IPv6 packets that it originates.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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

IPv6 packets that are originated from an unnumbered interface use the global IPv6 address of the interface specified in the **ipv6 unnumbered** command as the source address for the packets. The **ipv6 unnumbered** *interface* command is used as a hint when doing source address selection; that is, when trying to determine the source address of an outgoing packet.

Note Serial interfaces using High-Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), Frame Relay encapsulations, and tunnel interfaces can be unnumbered. You cannot use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.

Examples

The following example configures serial interface 0/1as unnumbered. IPv6 packets that are sent on serial interface 0/1 use the IPv6 address of Ethernet 0/0 as their source address:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 address 3FFE:C00:0:1:260:3EFF:FE11:6770
Router(config)# interface serial 0/1
Router(config-if)# ipv6 unnumbered ethernet 0/0
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 unreachables

To enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface, use the **ipv6 unreachables** command in interface configuration mode. To prevent the generation of unreachable messages, use the **no** form of this command.

ipv6 unreachables

no ipv6 unreachables

Syntax Description

This command has no arguments or keywords.

Command Default

ICMPv6 unreachable messages can be generated for any packets arriving on that interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)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

If the Cisco IOS software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMPv6 unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

Examples

The following example enables the generation of ICMPv6 unreachable messages, as appropriate, on an interface:

```
interface ethernet 0
 ipv6 unreachables
```

ipv6 verify unicast reverse-path

To enable Unicast Reverse Path Forwarding (Unicast RPF) for IPv6, use the **ipv6 verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ipv6 verify unicast reverse-path [**access-list** *name*]

no ipv6 verify unicast reverse-path [**access-list** *name*]

Syntax Description

access-list *name*	(Optional) Specifies the name of the access list. **Note** This keyword and argument are not supported on the Cisco 12000 series Internet router.

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S and introduced on the 10G Engine 5 SPA Interface Processor in the Cisco 12000 series Internet router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in strict checking mode. The Unicast RPF for IPv6 feature requires that Cisco Express Forwarding for IPv6 is enabled on the router.

Note Beginning in Cisco IOS Release 12.0(31)S, the Cisco 12000 series Internet router supports both the **ipv6 verify unicast reverse-path** and **ipv6 verify unicast source reachable-via rx** commands to enable Unicast RPF to be compatible with the Cisco IOS Release 12.3T and 12.2S software trains.

Use the **ipv6 verify unicast reverse-path** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source IPv6 address appears in the routing table and that it is reachable by a path through the interface on which the packet was received. Unicast RPF is an input feature and is applied only on the input interface of a router at the upstream end of a connection.

The Unicast RPF feature performs a reverse lookup in the CEF table to check if any packet received at a router interface has arrived on a path identified as a best return path to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast RPF command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast RPF command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Note When you configure Unicast RPF for IPv6 on the Cisco 12000 series Internet router, the most recently configured checking mode is not automatically applied to all interfaces as on other platforms. You must enable Unicast RPF for IPv6 separately on each interface. When you configure a SPA on the Cisco 12000 series Internet router, the interface address is in the format *slot/subslot/port*. The optional **access-list** keyword for the **ipv6 verify unicast reverse-path** command is not supported on the Cisco 12000 series Internet router. For information about how Unicast RPF can be used with ACLs on other platforms to mitigate the transmission of invalid IPv4 addresses (perform egress filtering) and to prevent (deny) the reception of invalid IPv4 addresses (perform ingress filtering), refer to the "Configuring Unicast Reverse Path Forwarding" chapter in the "Other Security Features" section of the *Cisco IOS Security Configuration Guide*.

Note When using Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on).

Do not use Unicast RPF on core-facing interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning that there are multiple routes to the source of a packet. Apply Unicast RPF only where there is natural or configured symmetry.

For example, routers at the edge of the network of an Internet service provider (ISP) are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Examples

Examples

The following example shows how to enable the Unicast RPF feature on a serial interface:

```
interface serial 5/0/0
  ipv6 verify unicast reverse-path
```

Examples

The following example shows how to enable Unicast RPF for IPv6 with strict checking on a 10G SIP Gigabit Ethernet interface 2/1/2:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitEthernet 2/1/2
Router(config-if)# ipv6 verify unicast reverse-path
Router(config-if)# exit
```

Examples

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 209.165.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
interface Serial 5/0/0
description Connection to Upstream ISP
ipv6 address FE80::260:3EFF:FE11:6770/64
no ipv6 redirects
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
permit ipv6 host 2::1 any
deny ipv6 FEC0::/10 any
  ipv6 access-group abc in
  ipv6 access-group jkl out
!
access-list abc permit ip FE80::260:3EFF:FE11:6770/64 2001:0DB8:0000:0001::0001any
access-list abc deny ipv6 any any log
access-list jkl deny ipv6 host 2001:0DB8:0000:0001::0001 any log
access-list jkl deny ipv6 2001:0DB8:0000:0001:FFFF:1234::5.255.255.255 any log
access-list jkl deny ipv6 2002:0EF8:002001:0DB8:0000:0001:FFFF:1234::5172.16.0.0
0.15.255.255 any log
access-list jkl deny ipv6 2001:0CB8:0000:0001:FFFF:1234::5 0.0.255.255 any log
access-list jkl deny ipv6 2003:0DB8:0000:0001:FFFF:1234::5 0.0.0.31 any log
access-list jkl permit ipv6
```

Examples

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL abc provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/0 to check packets arriving at that interface.

For example, packets with a source address of 8765:4321::1 arriving at Ethernet interface 0 are dropped because of the deny statement in ACL "abc." In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 1234:5678::1 arriving at Ethernet interface 0/0 are forwarded because of the permit statement

in ACL abc. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
interface ethernet 0/0
ipv6 address FE80::260:3EFF:FE11:6770/64 link-local
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
permit ipv6 1234:5678::/64 any log-input
deny ipv6 8765:4321::/64 any log-input
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.
ip verify unicast reverse-path	Enables Unicast RPF for IPv4 traffic.
ipv6 cef	Enables Cisco Express Forwarding for IPv6 interfaces.

ipv6 verify unicast source reachable-via

To verify that a source address exists in the FIB table and enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ipv6 verify unicast source reachable-via** command in interface configuration mode. To disable URPF, use the **no** form of this command.

ipv6 verify unicast source reachable-via {**rx**| **any**} **[allow-default] [allow-self-ping]** [*access-list-name*]

no ipv6 verify unicast

Syntax Description

rx	Source is reachable through the interface on which the packet was received.
any	Source is reachable through any interface.
allow-default	(Optional) Allows the lookup table to match the default route and use the route for verification.
allow-self-ping	(Optional) Allows the router to ping a secondary address.
access-list-name	(Optional) Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeral.

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in loose checking mode.

Use the **ipv6 verify unicast source reachable-via**command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through an IPv6 router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IPv6 address spoofing.

The URPF feature checks to see if any packet received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the CEF table. If URPF does not find a reverse path for the packet, U RPF can drop or forward the packet, depending on whether an access control list (ACL) is specified in the **ipv6 verify unicast source reachable-via** command. If an ACL is specified in the command, then when (and only when) a packet fails the URPF check, the ACL is checked to see if the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for U RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ipv6 verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

U RPF events can be logged by specifying the logging option for the ACL entries used by the **ipv6 verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Examples

The following example enables Unicast RPF on any interface:

```
ipv6 verify unicast source reachable-via any
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 virtual-reassembly

To enable Virtual Fragment Reassembly (VFR) on an interface, use the **ipv6 virtual-reassembly** command in global configuration mode. To remove VFR configuration, use the **no** form of this command.

ipv6 virtual-reassembly [**in**| **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] **[drop-fragments]**

no ipv6 virtual-reassembly [**in**| **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] **[drop-fragments]**

Syntax Description

in	(Optional) Enables VFR on the ingress direction of the interface.
out	(Optional) Enables VFR on the egress direction of the interface.
max-reassemblies *maxreassemblies*	(Optional) Sets the maximum number of concurrent reassemblies (fragment sets) that the Cisco IOS software can handle at a time. The default value is 64.
max-fragments *max-fragments*	(Optional) Sets the maximum number of fragments allowed per datagram (fragment set). The default is 16.
timeout *seconds*	(Optional) Sets the timeout value of the fragment state. The default timeout value is 2 seconds. If a datagram does not receive all its fragments within 2 seconds, all of the fragments received previously will be dropped and the fragment state will be deleted.
drop-fragments	(Optional) Turns the drop fragments feature on or off.

Command Default

Max-reassemblies = 64 Fragments = 16 If neither the **in** or **out** keyword is specified, VFR is enabled on the ingress direction of the interface only.**drop-fragments** keyword is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Release	Modification
15.1(1)T	The **in** and **out** keywords were added. • The **out** keyword must be used to configure or disable the egress direction of the interface.
Cisco IOS XE Release 3.4S	The **drop-fragments** keyword was added.

Usage Guidelines

When the **ipv6 virtual-reassembly** command is configured on an interface without using one of the command keywords, VFR is enabled on the ingress direction of the interface only. In Cisco IOS XE Release 3.4S, all VFR-related alert messages are suppressed by default.

Maximum Number of Reassemblies

Whenever the maximum number of 256 reassemblies (fragment sets) is crossed, all the fragments in the forthcoming fragment set will be dropped and an alert message VFR-4-FRAG_TABLE_OVERFLOW will be logged to the syslog server.

Maximum Number of Fragments per Fragment Set

If a datagram being reassembled receives more than eight fragments then, tall fragments will be dropped and an alert message VFR-4-TOO_MANY_FRAGMENTS will be logged to the syslog server.

Explicit Removal of Egress Configuration

As of the Cisco IOS 15.1(1)T release, the **no ipv6 virtual-reassembly** command, when used without keywords, removes ingress configuration only. To remove egress interface configuration, you must enter the **out** keyword.

Examples

The following example configures the ingress direction on the interface. It sets the maximum number of reassemblies to 32, maximum fragments to 4, and the timeout to 7 seconds:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly max-reassemblies 32 max-fragments 4 timeout 7
```

The following example enables the VFR on the ingress direction of the interface. Note that even if the **in** keyword is not used, the configuration default is to configure the ingress direction on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly
Router(config-if)# end
Router# show run interface Ethernet 0/0
interface Ethernet0/0
no ip address
ipv6 virtual-reassembly in
```

The following example enables egress configuration on the interface. Note that the **out** keyword must be used to enable and disable egress configuration on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly out
Router(config-if)# end
Router# show run interface Ethernet 0/0
interface Ethernet0/0
no ip address
ipv6 virtual-reassembly out
end
```

The following example disables egress configuration on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# no
 ipv6 virtual-reassembly out
Router(config-if)# end
```

ipv6 virtual-reassembly drop-fragments

To drop all fragments on an interface, use the **ipv6 virtual-reassembly drop-fragments** command in global configuration mode. Use the **no** form of this command to remove the packet-dropping behavior.

ipv6 virtual-reassembly drop-fragments

no ipv6 virtual-reassembly drop-fragments

Syntax Description

This command has no arguments or keywords.

Command Default

Fragments on an interface are not dropped.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example causes all fragments on an interface to be dropped:

```
ipv6 virtual-reassembly drop-fragments
```

ipv6 wccp

To enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **ipv6 wccp** command in global configuration mode. To disable the service group, use the **no** form of this command.

ipv6 wccp vrf *vrf-name* {**web-cache**| *service-number*} [**service-list** *service-access-list*] [**mode** {**open**| **closed**}] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [**0**| **7**] *password*]

no ipv6 wccp vrf *vrf-name* {**web-cache**| *service-number*} [**service-list** *service-access-list*] [**mode** {**open**| **closed**}] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [**0**| **7**] *password*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
web-cache	Specifies the web-cache service. **Note** Web cache is one of the services. The maximum number of services, including those assigned with the *service-number* argument, is 256.
service-number	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256, which includes the web-cache service specified with the **web-cache** keyword. **Note** If Cisco cache engines are being used in your service group, the reverse-proxy service is indicated by a value of 99.
service-list *service-access-list*	(Optional) Identifies a named extended IP access list that defines the packets that will match the service.
mode open	(Optional) Identifies the service as open. This is the default service mode.
mode closed	(Optional) Identifies the service as closed.
group-address *multicast-address*	(Optional) Specifies the multicast IP address that communicates with the WCCP service group. The multicast address is used by the router to determine which web cache should receive redirected messages.

redirect-list *access-list*	(Optional) Specifies the access list that controls traffic redirected to this service group. The *access-list* argument should consist of a string of no more than 64 characters (name or number) in length that specifies the access list.
group-list *access-list*	(Optional) Specifies the access list that determines which web caches are allowed to participate in the service group. The *access-list* argument specifies either the number or the name of a standard or extended access list.
password [**0** | **7**] *password*	(Optional) Specifies the message digest algorithm 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded. The encryption type can be 0 or 7, with 0 specifying not yet encrypted and 7 for proprietary. The *password* argument can be up to eight characters in length.

Command Default

WCCP services are not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwardin) switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the content engine interface, and specify the **ipv6 wccp web-cache redirect out** command. Configure WCCP in the incoming direction on the inside interface by specifying the **ipv6 wccp redirect exclude in** command on the router interface facing the cache. This configuration prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection.

This command instructs a router to enable or disable support for the specified service number or the web-cache service name. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

The **vrf** *vrf-name* keyword and argument pair is optional. It allows you to specify a VRF to associate with a service group. You can then specify a web-cache service name or service number.

The same service (web-cache or service number) can be configured in different VRF tables. Each service will operate independently.

When the **no ipv6 wccp** command is entered, the router terminates participation in the service group, deallocates space if none of the interfaces still has the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once. The following sections outline the specific usage of each of the optional forms of this command.

ipv6 wccp [vrf *vrf-name*] {web-cache | *service-number*} group-address *multicast-address*

A WCCP group address can be configured to set up a multicast address that cooperating routers and web caches can use to exchange WCCP protocol messages. If such an address is used, IP multicast routing must be enabled so that the messages that use the configured group (multicast) addresses are received correctly.

This option instructs the router to use the specified multicast IP address to coalesce the "I See You" responses for the "Here I Am" messages that it has received on this group address. The response also is sent to the group address. The default is for no group address to be configured, in which case all "Here I Am" messages are responded to with a unicast reply.

ipv6 wccp [vrf *vrf-name*] {web-cache | *service-number*} redirect-list *access-list*

This option instructs the router to use an access list to control the traffic that is redirected to the web caches of the service group specified by the service name given. The *access-list* argument specifies either the number or the name of a standard or extended access list. The access list itself specifies which traffic is permitted to be redirected. The default is for no redirect list to be configured (all traffic is redirected).

WCCP requires that the following protocol and ports not be filtered by any access lists:

- UDP (protocol type 17) port 2048. This port is used for control signaling. Blocking this type of traffic will prevent WCCP from establishing a connection between the router and web caches.
- Generic routing encapsulation (GRE) (protocol type 47 encapsulated frames). Blocking this type of traffic will prevent the web caches from ever seeing the packets that are intercepted.

ipv6 wccp [vrf *vrf-name*] {web-cache | *service-number*} group-list *access-list*

This option instructs the router to use an access list to control the web caches that are allowed to participate in the specified service group. The *access-list* argument specifies either the number of a standard or extended access list or the name of any type of named access list. The access list itself specifies which web caches are permitted to participate in the service group. The default is for no group list to be configured, in which case all web caches may participate in the service group.

Note The **ipv6 wccp** {**web-cache** | *service-number*} **group-list** command syntax resembles the **ipv6 wccp** {**web-cache** | *service-number*} **group-listen** command, but these are entirely different commands. The **ipv6 wccp group-listen** command is an interface configuration command used to configure an interface to listen for multicast notifications from a cache cluster. Refer to the description of the **ipv6 wccp group-listen** command in the *Cisco IOS IP Application Services Command Reference*.

ipv6 wccp [vrf *vrf-name*] web-cache | *service-number*} password *password*

This option instructs the router to use MD5 authentication on the messages received from the service group specified by the service name given. Use this form of the command to set the password on the router. You must also configure the same password separately on each web cache. The password can be up to a maximum of eight characters in length. Messages that do not authenticate when authentication is enabled on the router

are discarded. The default is for no authentication password to be configured and for authentication to be disabled.

ipv6 wccp *service-number* **service-list***service-access-list* **mode closed**

In applications where the interception and redirection of WCCP packets to external intermediate devices for the purpose of applying feature processing are not available within Cisco IOS software, it is necessary to block packets for the application when the intermediary device is not available. This blocking is called a closed service. By default, WCCP operates as an open service, wherein communication between clients and servers proceeds normally in the absence of an intermediary device. The **service-list** keyword can only be used for closed mode services. When a WCCP service is configured as closed, WCCP discards packets that do not have a client application registered to receive the traffic. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

When the definition of a service in a service list conflicts with the definition received via the WCCP protocol, a warning message similar to the following is displayed:

```
Sep 28 14:06:35.923: %WCCP-5-SERVICEMISMATCH: Service 90 mismatched on WCCP client 10.1.1.13
```

When there is a conflict in service list definitions, the configured definition takes precedence over the external definition received via WCCP protocol messages.

Examples

The following example shows how to configure a router to run WCCP reverse-proxy service, using the multicast address of 239.0.0.0:

```
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 wccp 99 group-address 239.0.0.0
Router(config)# interface ethernet 0
Router(config-if)# ipv6 wccp 99 group-listen
```

The following example shows how to configure a router to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

```
Router(config)# access-list 100 deny ip any host 10.168.196.51
Router(config)# access-list 100 permit ip any any
Router(config)# ipv6 wccp web-cache redirect-list 100
Router(config)# interface ethernet 0
Router(config-if)# ipv6 wccp web-cache redirect out
```

The following example shows how to configure an access list to prevent traffic from network 10.0.0.0 leaving Fast Ethernet interface 0/0. Because the outbound access control list (ACL) check is enabled, WCCP does not redirect that traffic. WCCP checks packets against the ACL before they are redirected.

```
Router(config)# ipv6 wccp web-cache
Router(config)# ipv6 wccp check acl outbound
Router(config)# interface fastethernet0/0
Router(config-if)# ip access-group 10 out
Router(config-if)# ipv6 wccp web-cache redirect out
Router(config-if)# access-list 10 deny 10.0.0.0 0.255.255.255
Router(config-if)# access-list 10 permit any
```

If the outbound ACL check is disabled, HTTP packets from network 10.0.0.0 would be redirected to a cache, and users with that network address could retrieve web pages when the network administrator wanted to prevent this from happening.

The following example shows how to configure a closed WCCP service:

```
Router(config)# ipv6 wccp 99 service-list access1 mode closed
```

Related Commands

Command	Description
ipv6 wccp check services all	Enables all WCCP services.
ipv6 wccp redirect excludein	Configures an interface to exclude packets received on an interface from being checked for redirection.
show ipv6 wccp	Displays global statistics related to WCCP.

ipv6 wccp check acl outbound

To check the access control list (ACL) for egress interfaces for packets redirected by the Web Cache Communication Protocol (WCCP), use the **ipv6 wccp check acl outbound** command in global configuration mode. To disable the outbound check for redirected packets, use the **no** form of this command.

ipv6 wccp check acl outbound

no ipv6 wccp check acl outbound

Syntax Description

This command has no arguments or keywords.

Command Default

Check of the outbound ACL services is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

This command enables the outbound check for redirected packets.

Examples

The following example shows how to configure a router to check the ACL for the egress interfaces for inbound packets that are redirected by WCCP:

```
Router(config)# ipv6 wccp check acl outbound
```

Related Commands

Command	Description
ipv6 wccp	Enables support of the specified WCCP service for participation in a service group.
ipv6 wccp check services all	Enables all WCCP services.

ipv6 wccpcheck services all

To enable all Web Cache Communication Protocol (WCCP) services, use the **ipv6 wccp check services all** command in global configuration mode. To disable all services, use the **no** form of this command.

ipv6 wccp check services all

no ipv6 wccp check services all

Syntax Description

This command has no arguments or keywords.

Command Default

WCCP services are not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

With the **ipv6 wccp check services all** command, WCCP can be configured to check all configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by a redirect access control list (ACL) and by the priority value of the service.

An interface can be configured with more than one WCCP service. When more than one WCCP service is configured on an interface, the precedence of a service depends on the relative priority of the service compared to the priority of the other configured services. Each WCCP service has a priority value as part of its definition.

If no WCCP services are configured with a redirect ACL, the services are considered in priority order until a service is found that matches the IP packet. If no services match the packet, the packet is not redirected. If a service matches the packet and the service has a redirect ACL configured, then the IP packet will be checked against the ACL. If the packet is rejected by the ACL, the packet will not be passed down to lower priority services unless the **ipv6 wccp check services all** command is configured. When the **ipv6 wccp check services all** command is configured, WCCP will continue to attempt to match the packet against any remaining lower priority services configured on the interface.

Note The priority of a WCCP service group is determined by the web cache appliance. The priority of a WCCP service group cannot be configured via Cisco IOS software.

Note The **ipv6 wccp check services all** command is a global WCCP command that applies to all services and is not associated with a single service.

Examples

The following example shows how to configure all WCCP services:

```
Router(config)# ipv6 wccp check services all
```

Related Commands

Command	Description
ipv6 wccp	Enables support of the specified WCCP service for participation in a service group.

ipv6 wccp group-listen

To configure an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP), use the **ipv6 wccp group-listen** command in interface configuration mode. To disable the reception of IP multicast packets for WCCP, use the **no** form of this command.

ipv6 wccp [**vrf** *vrf-name*] {**web-cache**| *service-number*} **group-listen**

no ipv6 wccp [**vrf** *vrf-name*] {**web-cache**| *service-number*} **group-listen**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
web-cache	Directs the router to send packets to the web cache service.
service-number	WCCP service number; valid values are from 0 to 254.

Command Default

No interface is configured to enable the reception of IP multicast packets for WCCP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

Note the following requirements on routers that are to be members of a service group when IP multicast is used:

- Configure the IP multicast address for use by the WCCP service group.
- Enable IP multicast routing using the **ipv6 multicast-routing** command in global configuration mode.
- Configure the interfaces on which the router wants to receive the IP multicast address with the **ipv6 wccp** {**web-cache** | *service-number*} **group-listen** interface configuration command.

Examples

The following example shows how to enable the multicast packets for a web cache with a multicast address of 2001:DB8:100::1:

```
Router# configure terminal
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 wccp web-cache group-address 2001:DB8:100::1
Router(config)# interface ethernet 0
Router(config-if)# ipv6 wccp web-cache group-listen
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing.
ipv6 wccp	Enables support of the WCCP service for participation in a service group.
ipv6 wccp redirect	Enables WCCP redirection on an interface.

ipv6 wccp redirect

To enable packet redirection on an outbound or inbound interface using the Web Cache Communication Protocol (WCCP), use the **ipv6 wccp redirect** command in interface configuration mode. To disable WCCP redirection, use the **no** form of this command.

ipv6 wccp [**vrf** *vrf-name*] {**web-cache**| *service-number*} **redirect** {**in**| **out**}

no ipv6 wccp [**vrf** *vrf-name*] {**web-cache**| *service-number*} **redirect** {**in**| **out**}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
web-cache	Enables the web cache service.
service-number	Identification number of the cache engine service group controlled by a router; valid values are from 0 to 254. If Cisco cache engines are used in the cache cluster, the reverse proxy service is indicated by a value of 99.
in	Specifies packet redirection on an inbound interface.
out	Specifies packet redirection on an outbound interface.

Command Default

Redirection checking on the interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the Content Engine interface, and specify the **ipv6 wccp web-cache redirect out** command. Configure WCCP in the incoming direction on the inside interface

by specifying the **ipv6 wccp redirect exclude in** command on the router interface facing the cache. This prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ipv6 wccp** command for configuration of the redirect list and service group.

The **ipv6 wccp redirect in** command allows you to configure WCCP redirection on an interface receiving inbound network traffic. When the command is applied to an interface, all packets arriving at that interface will be compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they will be redirected.

Likewise, the **ipv6 wccp redirect out** command allows you to configure the WCCP redirection check at an outbound interface.

Tip Be careful not to confuse the **ipv6 wccp redirect** {**out** | **in** } interface configuration command with the **ipv6 wccp redirect exclude in** interface configuration command.

Note This command has the potential to affect the **ipv6 wccp redirect exclude in** command. (These commands have opposite functions.) If you have **ipv6 wccp redirect exclude in** set on an interface and you subsequently configure the **ipv6 wccp redirect in** command, the **exclude in** command will be overridden. The opposite is also true: Configuring the **exclude in** command will override the **redirect in** command.

Examples

In the following configuration, the multilink interface is configured to prevent the bypassing of NAT when Cisco Express Forwarding switching is enabled:

```
Router(config)# interface multilink2
Router(config-if)# ipv6 address 2001:DB8:100::1 255.255.255.0
Router(config-if)# ip access-group IDS_Multilink2_in_1 in
Router(config-if)# ipv6 wccp web-cache redirect out
Router(config-if)# ipv6 nat outside
Router(config-if)# ipv6 inspect FSB-WALL out
Router(config-if)# max-reserved-bandwidth 100
Router(config-if)# service-policy output fsb-policy
Router(config-if)# no ip route-cache
Router(config-if)# load-interval 30
Router(config-if)# tx-ring-limit 3
Router(config-if)# tx-queue-limit 3
Router(config-if)# ids-service-module monitoring
Router(config-if)# ppp multilink
Router(config-if)# ppp multilink group 2
Router(config-if)# crypto map abc1
```

The following example shows how to configure a session in which reverse proxy packets on Ethernet interface 0 are being checked for redirection and redirected to a Cisco Cache Engine:

```
Router(config)# ipv6 wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ipv6 wccp 99 redirect out
```

The following example shows how to configure a session in which HTTP traffic arriving on Ethernet interface 0/1 is redirected to a Cisco Cache Engine:

```
Router(config)# ipv6 wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ipv6 wccp web-cache redirect in
```

Related Commands

Command	Description
ipv6 wccp redirect exclude in	Enables redirection exclusion on an interface.
show ipv6 interface	Displays the usability status of interfaces that are configured for IP.
show ipv6 wccp	Displays the WCCP global configuration and statistics.

ipv6 wccp redirect exclude in

To configure an interface to exclude packets received on an interface from being checked for redirection, use the **ipv6 wccp redirect exclude in** command in interface configuration mode. To disable the ability of a router to exclude packets from redirection checks, use the **no** form of this command.

ipv6 wccp redirect exclude in

no ipv6 wccp redirect exclude in

Syntax Description

This command has no arguments or keywords.

Command Default

Redirection exclusion is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

This configuration command instructs the interface to exclude inbound packets from any redirection check. Note that the command is global to all the services and should be applied to any inbound interface that will be excluded from redirection.

This command is intended to be used to accelerate the flow of packets from a cache engine to the Internet and to allow for the use of the WCCPv2 packet return feature.

Examples

In the following example, packets arriving on Ethernet interface 0 are excluded from all WCCP redirection checks:

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 wccp redirect exclude in
```

Related Commands

Command	Description
ipv6 wccp	Enables support of the WCCP service for participation in a service group.
ipv6 wccp redirect out	Configures redirection on an interface in the outgoing direction.

ipv6 wccp source-interface

To specify the interface that Web Cache Communication Protocol (WCCP) uses as the preferred router ID and generic routing encapsulation (GRE) source address, use the **ipv6 wccp source-interface** command in global configuration mode. To enable the WCCP default behavior for router ID selection, use the **no** form of this command.

ipv6 wccp [**vrf** *vrf-name*] **source-interface** *source-interface*

no ipv6 wccp [**vrf** *vrf-name*] **source-interface**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
source-interface	The type and number of the source interface.

Command Default

If this command is not configured, WCCP selects a loopback interface with the highest IP address as the router ID. If a loopback interface does not exist, then the interface that WCCP uses as the preferred router ID and GRE source address cannot be specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

Use this command to set the interface from which WCCP may derive the router ID and GRE source address. The router ID must be a reachable IPv6 address.

The interface identified by the *source-interface* argument must be assigned an IPv6 address and be operational before WCCP uses the address as the router ID. If the configured source interface cannot be used to derive the WCCP router ID, the configuration is ignored and a Cisco IOS error message similar to the following is displayed:

```
%WCCP-3-SIFIGNORED: source-interface interface
 ignored (reason)
```

The *reason* field in the error output indicates why the interface has been ignored and can include the following:

- **VRF mismatch**--The VRF domain associated with the interface does not match the VRF domain associated with the WCCP command.
- **interface does not exist**--The interface has been deleted.

- **no address**--The interface does not have a valid IPv6 address.
- **line protocol down**--The interface is not fully operational.

In the error case above, the source interface for the router ID will be selected automatically.

This command provides control only of the router ID and GRE source address. This command does not influence the source address used by WCCP control protocol (“Here I Am” and Removal Query messages). The WCCP control protocol is not bound to a specific interface and the source address is always selected based on the destination address of an individual packet.

Examples

The following example shows how to select Gigabit Ethernet interface 0/0/0 as the WCCP source interface:

```
Router(config)# ipv6 wccp source-interface gigabitethernet0/0/0
```

Related Commands

Command	Description
ipv6 wccp	Enables support of the specified WCCP service for participation in a service group.
show ipv6 wccp	Displays the WCCP global configuration and statistics.

isis ipv6 bfd

To enable or disable IPv6 Bidirectional Forwarding Detection (BFD) on a specific interface configured for Intermediate System-to-Intermediate System (IS-IS), use the **isis ipv6 bfd** command in interface configuration mode. To remove the IPv6 BFD configuration from the interface, use the **no** form of this command.

isis ipv6 bfd[disable]

noisis ipv6 bfd[disable]

Syntax Description

disable	(Optional) Disables IPv6 BFD for IS-IS on a specified interface.

Command Default

IPv6 BFD support for IS-IS is enabled on the interface.

Command Modes

Interface configuration (config-if)#

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Enter the **isis ipv6 bfd** command in interface configuration mode to configure an IS-IS interface to use IPv6 BFD for failure detection. If you have used the **bfd all-interfaces** command in router configuration mode to globally configure all IS-IS interfaces for an IS-IS process to use BFD, you can enter the **isis ipv6 bfd** command with the **disable** keyword in interface configuration mode to disable BFD for a specific IS-IS interface.

Entering the **no isis ipv6 bfd** command will remove the configuration from this IS-IS interface. In this case, whether or not an IS-IS interface for a particular IS-IS process is registered with the BFD protocol will depend on whether or not you have entered the **bfd all-interfaces** command in router configuration mode for the specific IS-IS process.

Examples

The following example enables IPv6 BFD on an IS-IS interface:

```
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# isis ipv6 bfd
```

Related Commands

Command	Description
ipv6 route priority high	Assigns a high priority to an IS-IS IPv6 prefix.
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another, using IS-IS as both the target and source protocol.
show isis database verbose	Displays additional information about the IS-IS database.
summary-prefix (IPv6 IS-IS)	Configures aggregate IPv6 prefixes for IS-IS.

isis ipv6 metric

To configure the value of an Intermediate System-to-Intermediate System (IS-IS) IPv6 metric, use the **is is ipv6 metric** command in interface configuration mode. To return the metric to its default value, use the **no** form of this command.

isis ipv6 metric {*metric-value*| **maximum**} [**level-1**| **level-2**]

no isis ipv6 metric {*metric-value*| **maximum**} [**level-1**| **level-2**]

Syntax Description

metric-value	Value added to the metric of an IPv6 IS-IS route received in a report message. The default metric value is 10. The range is from 1 to 16777214.
maximum	Excludes a link or adjacency from the Shortest Path Tree (SPF) calculation.
level-1	(Optional) Enables this command on routing Level 1. If no optional keyword is specified, the metric is enabled on routing Level 1 and Level 2.
level-2	(Optional) Enables this command on routing Level 2. If no optional keyword is specified, the metric is enabled on routing Level 1 and Level 2.

Command Default

The default metric value is set to 10.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.1	The **maximum** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **isis ipv6 metric** command is used only in multitopology IS-IS.

Changing the metric allows differentiation between IPv4 and IPv6 traffic, forcing traffic onto different interfaces. This function allows you to use the lower-cost rather than the high-cost interface.

For using extended metrics, such as with the IS-IS multitopology for IPv6 feature, Cisco IOS software provides support of a 24-bit metric field, the so-called "wide metric." Using the new metric style, link metrics now have a maximum value of 16777214 with a total path metric of 4261412864.

Cisco IOS Release 12.4(13) and 12.4(13)T

Entering the **maximum** keyword will exclude the link from the SPF calculation. If a link is advertised with the maximum link metric, the link will not be considered during the normal SPF computation. When the link excluded from the SPF, it will not be advertised for calculating the normal SPF. An example would be a link that is available for traffic engineering, but not for hop-by-hop routing. If a link, such as one that is used for traffic engineering, should not be included in the SPF calculation, enter the **isis ipv6 metric** command with the **maximum** keyword.

Note The **isis ipv6 metric maximum** command applies only when the **metric-style wide** command has been entered. The **metric-style wide**command is used to configure IS-IS to use the new-style type, length, value (TLV) because TLVs that are used to advertise IPv6 information in link-state packets (LSPs) are defined to use only extended metrics.

Examples

The following example sets the value of an IS-IS IPv6 metric to 20:

```
Router(config)# interface Ethernet 0/0/1
Router(config-if)# isis ipv6 metric 20
```

The following example sets the IS-IS IPv6 metric for the link to maximum. SPF will ignore the link for both Level 1 and Level 2 routing because neither the **level-1** keyword nor the **level-2** keyword was entered.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# isis ipv6 metric maximum
```

Related Commands

Command	Description
metric-style wide	Configures a router running IS-IS so that it generates and accepts only new-style TLVs.

isis ipv6 tag

To configure an administrative tag value that will be associated with an IPv6 address prefix and applied to an Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP), use the **isis ipv6 tag** command in interface configuration mode. To remove a tag from the address prefix, use the **no** form of this command.

isis ipv6 tag *tag-value*

no isis ipv6 tag

Syntax Description

tag-value	The tag value. The range is from 1 to 4294967295.

Command Default

An administrative IPv6 IS-IS tag is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

No action occurs on a tagged route until the tag is used, for example, to redistribute routes or summarize routes.

Configuring the **isis ipv6 tag** command triggers the router to generate new LSPs because the tag is a new piece of information in the packet.

Examples

In the following example, the value of an IS-IS IPv6 administrative tag is set to 220:

```
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# isis ipv6 tag 220
```

Related Commands

Command	Description
ipv6 route priority high	Assigns a high priority to an IS-IS IPv6 prefix.

Command	Description
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another, using IS-IS as both the target and source protocol.
show isis database verbose	Displays additional information about the IS-IS database.
summary-prefix (IPv6 IS-IS)	Configures aggregate IPv6 prefixes for IS-IS.

limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the **limit address-count**command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode .

limit address-count *maximum*

Syntax Description

maximum	Sets the role of the device to host.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration (config-nd-inspection) RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **limit address-count** command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size.

Use the **limit address-count**command after enabling NDP inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and limits the number of IPv6 addresses allowed on the port to 25:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# limit address-count 25
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy n ame and enters NDP inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

log-adjacency-changes (OSPFv3)

To configure the router to send a syslog message when an Open Shortest Path First version 3 (OSPFv3) neighbor goes up or down, use the **log-adjacency-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

log-adjacency-changes [detail]

no log-adjacency-changes [detail]

Syntax Description

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

Command Default

This feature is enabled

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use the **log-adjacency changes** command to notify you when OSPFv3 neighbors go up or down. The **log-adjacency-changes** command provides a higher level view of those changes of the peer relationship with less output than **debug** commands provide. The **log-adjacency-changes** command is on by default, but only up/down (full/down) events are reported unless the **detail** keyword is also used.

Examples

The following example configures the router to send a syslog message when an OSPFv3 neighbor state changes:

```
Router(config-router)# log-adjacency-changes
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

log-neighbor-changes (IPv6 EIGRP)

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 neighbor adjacencies, use the **log-neighbor-changes** command in router configuration mode. To disable the logging of changes in EIGRP IPv6 neighbor adjacencies, use the **no** form of this command.

log-neighbor-changes

no log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Adjacency changes are logged.

Command Modes

Router configuration

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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The log-neighbor-changes command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.

Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the no form of this command.

Examples

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

```
ipv6 router eigrp 1
 no log-neighbor-changes
```

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

```
ipv6 router eigrp 1
 log-neighbor-changes
```

Related Commands

Command	Description
log-neighbor- warnings	Enables the logging of EIGRP neighbor warning messages.

managed-config-flag

To verify the advertised managed address configuration parameter, use the **managed-config-flag** command in RA guard policy configuration mode.

managed-config-flag {**on**| **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **managed-config-flag** command enables verification of the advertised managed address configuration parameter (or "M" flag). This flag could be set by an attacker to force hosts to obtain addresses through a DHCPv6 server that may not be trustworthy.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables M flag verification:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# managed-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

match access-group name

To specify the name of an IPv6 access list against whose contents packets are checked to determine if they belong to the traffic class, use the **match access-group name** command in class-map configuration mode. To remove the name of the IPv6 access list, use the **no** form of this command.

match access-group name *ipv6-access-group*

no match access-group name *ipv6-access-group*

Syntax Description

ipv6-access-group	Name of the IPv6 access group. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series routers.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including access control lists (ACLs), protocols, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match access-group name** command specifies an IPv6 named ACL only. The contents of the ACL are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match access-group name** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match dscp**
- **match mpls experimental**
- **match precedence**

- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

Examples

The following example specifies an access list named ipv6acl against whose contents packets will be checked to determine if they belong to the traffic class:

```
class-map ipv6_acl_class
match access-group name ipv6acl
```

Related Commands

Command	Description
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match dscp	Identifies a specific IP DSCP value as a match criterion.
match mpls experimental	Configures a class map to use the specified value of the experimental (EXP) field as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match identity

To match an identity from a peer in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **match identity**command in ISAKMP profile configuration mode. To remove the identity, use the **no** form of this command.

match identity {**group** *group-name*| **address** {*address* [*mask*] [*fvrf*]| **ipv6** *ipv6-address*}| **host** *host-name*| **host domain** *domain-name*| **user** *user-fqdn*| **user domain** *domain-name*}

no match identity {**group** *group-name*| **address** {*address* [*mask*] [*fvrf*]| **ipv6** *ipv6-address*}| **host** *host-name*| **host domain** *domain-name*| **user** *user-fqdn*| **user domain** *domain-name*}

Syntax Description

group *group-name*	A Unity group that matches identification (ID) type ID_KEY_ID. If Unity and main mode Rivest, Shamir, and Adelman (RSA) signatures are used, the *group-name* argument matches the Organizational Unit (OU) field of the Distinguished Name (DN).
address *address* [*mask*] [*fvrf*]	Identity that matches the identity of type ID_IPV4_ADDR. • *mask*-- Use to match the range of the address. • *fvrf* --Use to match the address in the front door Virtual Route Forwarding (FVRF) Virtual Private Network (VPN) space.
ipv6 *ipv6-address*	Identity that matches the identity of type ID_IPV6_ADDR.
host *host-name*	Identity that matches an identity of the type ID_FQDN.
host domain *domain-name*	Identity that matches an identity of the type ID_FQDN, whose fully qualified domain name (FQDN) ends with the domain name.
user *user-fqdn*	Identity that matches the FQDN.
user domain *domain-name*	Identity that matches the identities of the type ID_USER_FQDN. When the **user domain** keyword is present, all users having identities of the type ID_USER_FQDN and ending with "*domain-name*" will be matched.

Command Default

No default behavior or values

Command Modes

ISAKMP profile configuration (conf-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **ipv6** keyword and *ipv6-address a*rgument were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

There must be at least one **match identity**command in an ISAKMP profile configuration. The peers are mapped to an ISAKMP profile when their identities are matched (as given in the ID payload of the Internet Key Exchange [IKE] exchange) against the identities that are defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid.

Examples

The following example shows that the **match identity**command is configured:

```
crypto isakmp profile vpnprofile
 match identity group vpngroup
 match identity address 10.53.11.1
 match identity host domain example.com
 match identity host server.example.com
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.

match ipv6

To configure one or more of the IPv6 fields as a key field for a flow record, use the **match ipv6** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the IPv6 fields as a key field for a flow record, use the **no** form of this command.

match ipv6 {**dscp**| **flow-label**| **next-header**| **payload-length**| **precedence**| **protocol**| **traffic-class**| **version**}

no match ipv6 {**dscp**| **flow-label**| **next-header**| **payload-length**| **precedence**| **protocol**| **traffic-class**| **version**}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

match ipv6 {**dscp**| **precedence**| **protocol**| **tos**}

no match ipv6 {**dscp**| **precedence**| **protocol**| **tos**}

Cisco IOS XE Release 3.2SE

match ipv6 {**protocol**| **traffic-class**| **version**}

no match ipv6 {**protocol**| **traffic-class**| **version**}

Syntax Description

dscp	Configures the IPv6 differentiated services code point DSCP (part of type of service (ToS)) as a key field.
flow-label	Configures the IPv6 flow label as a key field.
next-header	Configures the IPv6 next header as a key field.
payload-length	Configures the IPv6 payload length as a key field.
precedence	Configures the IPv6 precedence (part of ToS) as a key field.
protocol	Configures the IPv6 protocol as a key field.
tos	Configures the IPv6 ToS as a key field.
traffic-class	Configures the IPv6 traffic class as a key field.
version	Configures the IPv6 version from IPv6 header as a key field.

Command Default

The IPv6 fields are not configured as a key field.

Command Modes

Flexible Netflow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was modified. Support for this command was implemented on the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
12.2(50)SY	This command was modified. The **flow-label**, **next-header**, **payload-length,traffic-class**, and **version** keywords were removed.
15.2(2)T	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.5S	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.2SE	This command was modified. The **dscp**, **flow-label**, **next-header**, **payload-length**, and **precedence** keywords were removed.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Note Some of the keywords of the **match ipv6** command are documented as separate commands. All of the keywords for the **match ipv6** command that are documented separately start with **match ipv6**. For example, for information about configuring the IPv6 hop limit as a key field for a flow record, refer to the **match ipv6 hop-limit** command.

Examples

The following example configures the IPv6 DSCP field as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 dscp
```

The following example configures the IPv6 DSCP field as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 dscp
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 access-list

To verify the sender's IPv6 address in inspected messages from the authorized prefix list, use the **match ipv6 access-list** command in RA guard policy configuration mode.

match ipv6 access-list *ipv6-access-list-name*

Syntax Description

ipv6-access-list-name	The IPv6 access list to be matched.

Command Default

Senders' IPv6 addresses are not verified.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **match ipv6 access-list** command enables verification of the sender's IPv6 address in inspected messages from the configured authorized router source access list. If the **match ipv6 access-list** command is not configured, this authorization is bypassed.

An access list is configured using the **ipv6 access-list** command. For instance, to authorize the router with link-local address FE80::A8BB:CCFF:FE01:F700 only, define the following IPv6 access list:

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any
```

Note The access list is used here as a convenient way to define several explicit router sources, but it should not be considered to be a port-based access list (PACL). The **match ipv6 access-list** command verifies the IPv6 source address of the router messages, so specifying a destination in the access list is meaningless and the destination of the access control list (ACL) entry should always be "any." If a destination is specified in the access list, then matching will fail.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and matches the IPv6 addresses in the access list named list1:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ipv6 access-list list1
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.

match ipv6 address

To distribute IPv6 routes that have a prefix permitted by a prefix list or to specify an IPv6 access list to be used to match packets for policy-based routing (PBR) for IPv6, use the **match ipv6 address** command in route-map configuration mode. To remove the **match ipv6 address** entry, use the **no** form of this command.

match ipv6 address {**prefix-list** *prefix-list-name*| *access-list-name*}

no match ipv6 address

Syntax Description

prefix-list *prefix-list-name*	Specifies the name of an IPv6 prefix list.
access-list-name	Name of the IPv6 access list. Names cannot contain a space or quotation mark or begin with a numeric.

Command Default

No routes are distributed based on the destination network number or an access list.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.3(7)T	This command was modified. The *access-list-name* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SXI4	This command was modified. The **prefix-list** *prefix-list-name* keyword-argument pair argument is not supported in Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **route-map** command and the **match** and **set** commands to define the conditions for redistributing routes from one routing protocol to another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria--the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions, which are the particular redistribution actions to be performed if the criteria enforced by the **match** commands are met.

The **match ipv6 address** command can be used to specify either an access list or a prefix list. When using PBR, you must use the *access-list-name* argument; the **prefix-list** *prefix-list-name* keyword-argument pair argument will not work.

Examples

In the following example, IPv6 routes that have addresses specified by the prefix list named marketing are matched:

```
Device(config)# route-map name
Device(config-route-map)# match ipv6 address prefix-list marketing
```

In the following example, IPv6 routes that have addresses specified by an access list named marketing are matched:

```
Device(config)# route-map
Device(config-route-map)# match ipv6 address marketing
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Specifies an IPv6 access list to be used to match packets for PBR for IPv6.
match ipv6 next-hop	Distributes IPv6 routes that have a next-hop prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.
match length	Bases policy routing on the Level 3 length of a packet.
match metric	Redistributes routes with the specified metric.
match route-type	Redistributes routes of the specified type.
route-map	Defines conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP community attribute.

Command	Description
set default interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.
set level	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ipv6 destination

To configure the IPv6 destination address as a key field for a flow record, use the **match ipv6 destination** command in Flexible Netflow flow record configuration mode. To disable the IPv6 destination address as a key field for a flow record, use the **no** form of this command.

match ipv6 destination {**address**| {**mask**| **prefix**} [**minimum-mask** *mask*]}

no match ipv6 destination {**address**| {**mask**| **prefix**} [**minimum-mask** *mask*]}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

match ipv6 destination address

no match ipv6 destination address

Cisco IOS XE Release 3.2SE

match ipv6 destination address

no match ipv6 destination address

Syntax Description

address	Configures the IPv6 destination address as a key field.
mask	Configures the mask for the IPv6 destination address as a key field.
prefix	Configures the prefix for the IPv6 destination address as a key field.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 128.

Command Default

The IPv6 destination address is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was modified. Support for this command was implemented on the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Release	Modification
12.2(50)SY	This command was modified. The **mask**, **prefix**, and **minimum-mask** keywords were removed.
15.2(2)T	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.5S	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.2SE	This command was modified. The **mask**, **prefix**, and **minimum-mask** keywords were removed.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures a 16-bit IPv6 destination address prefix as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination prefix minimum-mask 16
```

The following example specifies a 16-bit IPv6 destination address mask as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination mask minimum-mask 16
```

The following example configures a 16-bit IPv6 destination address mask as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 destination mask minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 extension map

To configure the bitmap of the IPv6 extension header map as a key field for a flow record, use the **match ipv6 extension map** command in flow record configuration mode. To disable the use of the IPv6 bitmap of the IPv6 extension header map as a key field for a flow record, use the **no** form of this command.

match ipv6 extension map

no match ipv6 extension map

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the bitmap of the IPv6 extension header map as a key field for a user-defined flow record is not enabled by default.

Command Modes

Flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T for Cisco Performance Monitor.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Bitmap of the IPv6 Extension Header Map

The bitmap of IPv6 extension header map is made up of 32 bits.

```
    0     1     2     3     4     5     6     7
+-----+-----+-----+-----+-----+-----+-----+-----+
| Res | FRA1| RH  | FRA0| UNK | Res | HOP | DST |
+-----+-----+-----+-----+-----+-----+-----+-----+
    8     9    10    11    12    13    14    15
+-----+-----+-----+-----+-----+-----+-----+-----+
| PAY | AH  | ESP |          Reserved           |
+-----+-----+-----+-----+-----+-----+-----+-----+
   16    17    18    19    20    21    22    23
+-----+-----+-----+-----+-----+-----+-----+-----+
|                  Reserved                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
   24    25    26    27    28    29    30    31
+-----+-----+-----+-----+-----+-----+-----+-----+
|                  Reserved                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
0  Res  Reserved
1  FRA1 Fragmentation header - not first fragment
2  RH   Routing header
3  FRA0 Fragment header - first fragment
4  UNK  Unknown Layer 4 header
        (compressed, encrypted, not supported)
5  Res  Reserved
6  HOP  Hop-by-hop option header
7  DST  Destination option header
8  PAY Payload compression header
9  AH  Authentication Header
10 ESP Encrypted security payload
11 to 31 Reserved
```

For more information on IPv6 headers, refer to RFC 2460 *Internet Protocol, Version 6 (IPv6)* at the following URL: http://www.ietf.org/rfc/rfc2460.txt .

Examples

The following example configures the IPv6 bitmap of the IPv6 extension header map of the packets in the flow as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 extension map
```

Examples

The following example configures the IPv6 bitmap of the IPv6 extension header map of the packets in the flow as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 extension map
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 fragmentation

To configure one or more of the IPv6 fragmentation fields as a key field for a flow record, use the **match ipv6 fragmentation** command in flow record configuration mode. To disable the use of the IPv6 fragmentation field as a key field for a flow record, use the **no** form of this command.

match IPv6 fragmentation {**flags**| **id**| **offset**}

no match IPv6 fragmentation {**flags**| **id**| **offset**}

Syntax Description

flags	Configures the IPv6 fragmentation flags as a key field.
id	Configures the IPv6 fragmentation ID as a key field.
offset	Configures the IPv6 fragmentation offset value as a key field.

Command Default

The IPv6 fragmentation field is not configured as a key field.

Command Modes

Flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T for Cisco Performance Monitor.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible

NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the IPv6 fragmentation flags a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 fragmentation flags
```

The following example configures the IPv6 offset value a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 fragmentation offset
```

Examples

The following example configures the IPv6 offset value as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 fragmentation offset
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 hop-limit

To configure the IPv6 hop limit as a key field for a flow record, use the **match ipv6 hop-limit** command in Flexible NetFlow flow record configuration mode. To disable the use of a section of an IPv6 packet as a key field for a flow record, use the **no** form of this command.

match ipv6 hop-limit

no match ipv6 hop-limit

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the IPv6 hop limit as a key field for a user-defined flow record is not enabled by default.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was modified. Support for this command was implemented on the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
15.2(2)T	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.5S	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the hop limit of the packets in the flow as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 hop-limit
```

The following example configures the hop limit of the packets in the flow as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 hop-limit
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 length

To configure one or more of the IPv6 length fields as a key field for a flow record, use the **match ipv6 length** command in flow record configuration mode. To disable the use of the IPv6 length field as a key field for a flow record, use the **no** form of this command.

match ipv6 length {**header**| **payload**| **total**}

no match ipv6 length {**header**| **payload**| **total**}

Syntax Description

header	Configures the length in bytes of the IPv6 header, not including any extension headers as a key field.
payload	Configures the length in bytes of the IPv6 payload, including any extension header as a key field.
total	Configures the total length in bytes of the IPv6 header and payload as a key field.

Command Default

The IPv6 length field is not configured as a key field.

Command Modes

Flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T for Cisco Performance Monitor.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the length of the IPv6 header in bytes, not including any extension headers, as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 length header
```

Examples

The following example configures the length of the IPv6 header in bytes, not including any extension headers, as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 length header
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 next-hop

To distribute IPv6 routes that have a next hop prefix permitted by a prefix list, use the **match ipv6 next-hop** command in route-map configuration mode. To remove the **match ipv6 next-hop** entry, use the **no** form of this command.

match ipv6 next-hop prefix-list *prefix-list-name*

no match ipv6 next-hop

Syntax Description

prefix-list *prefix-list-name*	Name of an IPv6 prefix list.

Command Default

Routes are distributed freely, without being required to match a next hop address.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 **match ipv6 next-hop**command is similar to the **match ip next-hop**command, except that it is IPv6-specific.

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

The **match** command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions*given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** command relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Note A permit route map containing only **set** commands and no **match** commands permits all routes.

Examples

The following example distributes routes that have a next hop IPv6 address passed by the prefix list named marketing:

```
Router(config)# route-map name
Router(config-route-map)# match ipv6 next-hop prefix-list marketing
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.
match metric	Redistributes routes with the metric specified.
match route-type	Redistributes routes of the specified type.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP community attribute.
set level	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.

Command	Description
set metric-type	Sets the metric type for the destination routing protocol.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ipv6 route-source

To distribute IPv6 routes that have been advertised by routers at an address specified by a prefix list, use the **match ipv6 route-source** command in route-map configuration mode. To remove the **match ipv6 route-source** entry, use the **no** form of this command.

match ipv6 route-source prefix-list *prefix-list-name*

no match ipv6 route-source

Syntax Description

prefix-list *prefix-list-name*	Name of an IPv6 prefix list.

Command Default

No filtering on route source.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 **match ipv6 route-source**command is similar to the **match ip route-source** command, except that it is IPv6-specific.

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

The **match** command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions*given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** command relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

There are situations in which the next hop for a route and the source networking device address are not the same.

Note A permit route map containing only **set** commands and no **match** commands permits all routes.

Examples

The following example distributes routes that have been advertised by networking devices at the addresses specified by the prefix list named marketing:

```
Router(config)# route-map name
Router(config-route-map)# match ipv6 route-source prefix-list marketing
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
match ipv6 next-hop	Distributes IPv6 routes that have a next hop prefix permitted by a prefix list.
match metric	Redistributes routes with the metric specified.
match route-type	Redistributes routes of the specified type.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP community attribute.
set level	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.

Command	Description
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ra prefix-list

To verify the advertised prefixes in inspected messages from the authorized prefix list, use the **match ra prefix-list** command in RA guard policy configuration mode.

match ra prefix-list *ipv6-prefix-list-name*

Syntax Description

ipv6-prefix-list-name	The IPv6 prefix list to be matched.

Command Default

Advertised prefixes are not verified.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **match ra prefix-list** command enables verification of the advertised prefixes in inspected messages from the configured authorized prefix list. Use the **ipv6 prefix-list** command to configure an IPv6 prefix list. For instance, to authorize the 2001:101::/64 prefixes and deny the 2001:100::/64 prefixes, define the following IPv6 prefix list:

```
Router(config)# ipv6 prefix-list listname1 deny 2001:0DB8:101:/64
Router(config)# ipv6 prefix-list listname1 permit 2001:0DB8:100::/64
```

Examples

The following example shows how the command defines an router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and verifies the advertised prefixes in listname1:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ra prefix-list listname1
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.

maximum-paths (IPv6)

To control the maximum number of equal-cost routes that a process for IPv6 Border Gateway Protocol (BGP), a process for IPv6 Intermediate System-to-Intermediate System (IS-IS), a process for IPv6 Routing Information Protocol (RIP), a process for Open Shortest Path First (OSPF) for IPv6, or a process for Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing can support, use the **maximum-paths**command in address family configuration or router configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number-paths*

no maximum-paths

Syntax Description

number-paths	Maximum number of equal-cost paths to a destination learned via IPv6 BGP, IS-IS, RIP, OSPF, or EIGRP installed in the IPv6 routing table, in the range from 1 to 64.

Command Default

The default for BGP is 1 path, the default for IS-IS and RIP is 4 paths, and the default for OSPF for IPv6 is 16 paths .

Command Modes

Address family configuration Router configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S and support for IPv6 RIP was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	Support for IPv6 OSPF was added.
12.4(6)T	Support for EIGRP for IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To configure the **maximum-paths**command for IPv6 BGP and IS-IS, enter address family configuration mode.

Examples

The following example shows a maximum of three paths to an external destination for the IPv6 BGP autonomous system 65000, and a maximum of two paths to an IPv6 internal BGP destination being configured:

```
Router(config)# router bgp 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# maximum-paths 3
Router(config-router-af)# maximum-paths ibgp 2
```

The following example shows a maximum of two paths to a destination for the IPv6 IS-IS routing process named area01 being configured:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# maximum-paths 2
```

The following example shows a maximum of one path to a destination for the IPv6 RIP routing process named one being configured:

```
Router(config)# ipv6 router rip one
Router(config-router-rip)# maximum-paths 1
```

The following example shows a maximum of four paths to a destination for an IPv6 OSPF routing process:

```
Router(config) ipv6 router ospf 1
Router(config-router)# maximum-paths 4
```

The following example shows a maximum of two paths to a destination for an EIGRP for IPv6 routing process:

```
Router(config) ipv6 router eigrp 1
Router(config-router)# maximum-paths 2
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
ipv6 router eigrp	Configures the EIGRP routing process in IPv6.
ipv6 router ospf	Enables OSPF for IPv6 router configuration mode.
ipv6 router rip	Configures an IPv6 RIP routing process.
router bgp	Configures the BGP routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

maximum-paths (OSPFv3)

To control the maximum number of equal-cost routes that a process for Open Shortest Path First version 3 (OSPFv3) routing can support, use the **maximum-paths**command in IPv6 or IPv4 address family configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number-paths*

no maximum-paths

Syntax Description

number-paths	Maximum number of equal-cost paths to a destination learned through OSPFv3. The range is from 1 through 64.

Command Default

16 equal-cost paths

Command Modes

IPv6 address family configuration (config-router-af) IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command is used to control the maximum number of equal-cost routes that a process for OSPFv3 routing can support.

Examples

The following example shows how to configure a maximum of four paths to a destination for an OSPFv3 routing process:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# maximum-paths 4
```

mls ipv6 acl compress address unicast

To enable the compression of compressible IPv6 addresses, use the **mls ipv6 acl compress address unicast** command in global configuration mode. To disable the compression of compressible IPv6 addresses, use the **no** form of this command.

mls ipv6 acl compress address unicast

no mls ipv6 acl compress address unicast

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Note Do not enable the compression mode if you have noncompressible address types in your network. Compressible address types and the address compression method are listed in the table below.

Table 1: Compressible Address Types and Methods

Address Type	Compression Method
EUI-64 based on MAC address	This address is compressed by removing 16 bits from bit locations [39:24]. No information is lost when the hardware compresses these addresses.
Embedded IPv4 address	This address is compressed by removing the upper 16 bits. No information is lost when the hardware compresses these addresses.

Address Type	Compression Method
Link Local	These addresses are compressed by removing the zeros in bits [95:80] and are identified using the same packet type as the embedded IPv4 address. No information is lost when the hardware compresses these addresses.
Other	If the IPv6 address does not fall into any of the categories, it is classified as Other. If the IPv6 address is classified as Other, the following occurs: • If the compress mode is on, the IPv6 address is compressed similarly to the EUI-64 compression method (removal of bits [39:24]) to allow for the Layer 4 port information to be used as part of the key used to look up the quality of service (QoS) ternary content addressable memory (TCAM), but Layer 3 information is lost. • If the global compression mode is off, the entire 128 bits of the IPv6 address are used. The Layer 4 port information cannot be included in the key to look up the QoS TCAM because of the size constraints on the IPv6 lookup key.

Examples

This example shows how to turn on the compression of compressible IPv6 addresses:

```
Router(config)#
mls ipv6 acl compress address unicast
```

This example shows how to turn off the compression of compressible IPv6 addresses:

```
Router(config)#
no mls ipv6 acl compress address unicast
```

Related Commands

Command	Description
show fm ipv6 traffic-filter	Displays the IPv6 information.
show mls netflow ipv6	Displays configuration information about the NetFlow hardware.

mls ipv6 acl source

To deny all IPv6 packets from a source-specific address, use the **mls ipv6 acl source**command in global configuration mode. To accept all IPv6 packets from a source-specific address, use the **no** form of this command.

mls ipv6 acl source {**loopback**| **multicast**}

no mls ipv6 acl source {**loopback**| **multicast**}

Syntax Description

loopback	Denies all IPv6 packets with a source loopback address .
multicast	Denies all IPv6 packets with a source multicast address.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17b)SXA	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to deny all IPv6 packets with a source loopback address:

```
Router(config)#
mls ipv6 acl source loopback
```

This example shows how to deny all IPv6 packets with a source multicast address:

```
Router(config)#
no mls ipv6 acl source multicast
```

Related Commands

Command	Description
show mls netflow ipv6	Displays configuration information about the NetFlow hardware.

mls ipv6 slb search wildcard rp

To specify the behavior of Server Load Balancing (SLB) wildcard searches by the route processor (RP), use the **mls ipv6 slb search wildcard rp** command in global configuration mode. To restore the default setting, use the **no** form of this command.

mls ipv6 slb search wildcard rp

no mls ipv6 slb search wildcard rp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.2(4)S	This command was introduced on the Cisco 7600 Series devices.

Usage Guidelines

This command is supported for Cisco 7600 Series devices only.

Examples

The following example shows how to configure the SLB wildcard searches:

```
Router(config)# mls ipv6 slb search wildcard rp
```

Related Commands

Command	Description
ip slb firewallfarm	Identifies a firewall by IP address farm and enters firewall farm configuration mode.
ip slb serverfarm	Associates a real server farm with a virtual server.
ip slb vserver	Identifies a virtual server.

mls ipv6 vrf

To enable IPv6 globally in a virtual routing and forwarding (VRF) instance, use the mls ipv6 vrf command in global configuration mode. To remove this functionality, use the no form of the command.

mls ipv6 vrf

no mls ipv6 vrf

Syntax Description

This command has no arguments or keywords.

Command Default

VRFs are supported only for IPv4 addresses.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB1	This command was introduced on the Cisco 7600 series routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI and implemented on the Catalyst 6500 series switches.
Cisco IOS XE Release 3.1S	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

You must enable the mls ipv6 vrf command in global configuration mode in order to enable IPv6 in a VRF. If this command is not used, a VRF is supported only for the IPv4 address family.

Configuring the mls ipv6 vrf command makes the router reserve the lower 255 hardware IDs for IPv6 regardless of whether IPv6 is enabled. Other applications that make use of these hardware IDs then cannot use that space.

To remove the **mls ipv6 vrf** command from the running configuration, the user needs to remove all IPv6 VRFs from the router and reload the system.

Examples

The following example shows how to enable IPv6 in a VRF globally:

```
Router(config)# mls ipv6 vrf
```

Related Commands

Command	Description
vrf definition	Configure a VRF routing table instance and enters VRF configuration mode.

Command	Description
show running-config vrf	Displays the subset of the running configuration of a router that is linked to a specific VRF instance or to all VRFs configured on the router.

mls rate-limit multicast ipv6

To configure the IPv6 multicast rate limiters, use the **mls rate-limit multicast ipv6**command in global configuration mode. To disable the rate limiters, use the **no** form of this command.

mls rate-limit multicast ipv6 {**connected pps [packets-in-burst]**| **rate-limiter-name share** {**auto**| **target-rate-limiter**}}

no mls rate-limit multicast ipv6 {**connected**| *rate-limiter-name*}

Syntax Description

connected *pps*	Enables and sets the rate limiters for the IPv6 multicast packets from a directly connected source ; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
rate-limiter-name	Rate-limiter name; valid values are default-drop , route-cntl , secondary-drop , sg , starg-bridge , and starg-m-bridge . See the “Usage Guidelines” section for additional information.
share	Specifies the sharing policy for IPv6 rate limiters; see the “Usage Guidelines” section for additional information.
auto	Decides the sharing policy automatically.
target-rate-limiter	Rate-limiter name that was the first rate-limiter name programmed in the hardware for the group; valid values are default-drop , route-cntl , secondary-drop , sg , starg-bridge , and starg-m-bridge . See the “Usage Guidelines” section for additional information.

Command Default

If the *burst* is not set, a default of **100** is programmed for multicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The *rate-limiter-name*argument must be a rate limiter that is not currently programmed.

The *target-rate-limiter*argument must be a rate limiter that is programmed in the hardware and must be the first rate limiterprogrammed for its group.

The table below lists the IPv6 rate limiters and the class of traffic that each rate limiter serves.

Table 2: IPv6 Rate Limiters

Rate-Limiter ID	Traffic Classes to be Rate Limited
Connected	Directly connected source traffic
Default-drop	* (*, G/m)SSM * (*, G/m)SSM non-rpf
Route-control	* (*, FF02::X/128)
Secondary-drop	* (*, G/128) SPT threshold is infinity
SG	* (S, G) RP-RPF post-switchover * (*, FFx2/16)
Starg-bridge	* (*, G/128) SM * SM non-rpf traffic when (*, G) exists
Starg-M-bridge	* (*, G/m) SM * (*, FF/8) * SM non-rpf traffic when (*, G) does not exist

You can configure rate limiters for IPv6 multicast traffic using one of the following methods:

- Direct association of the rate limiters for a traffic class--Select a rate and associate the rate with a rate limiter. This example shows how to pick a rate of 1000 pps and 20 packets per burst and associate the rate with the **default-drop** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

- Static sharing of a rate limiter with another preconfigured rate limiter--When there are not enough adjacency-based rate limiters available, you can share a rate limiter with an already configured rate limiter (target rate limiter). This example shows how to share the **route-cntl** rate limiter with the **default-drop** target rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
```

If the target rate limiter is not configured, a message displays that the target rate limiter must be configured for it to be shared with other rate limiters.

- Dynamic sharing of rate limiters--If you are not sure about which rate limiter to share with, use the **share auto** keywords to enable dynamic sharing. When you enable dynamic sharing, the system picks a preconfigured rate limiter and shares the given rate limiter with the preconfigured rate limiter. This example shows how to choose dynamic sharing for the **route-cntrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
```

Examples

This example shows how to set the rate limiters for the IPv6 multicast packets from a directly connected source:

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
Router(config)#
```

This example shows how to configure a direct association of the rate limiters for a traffic class:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
Router(config)#
```

This example shows how to configure the static sharing of a rate limiter with another preconfigured rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
Router(config)#
```

This example shows how to enable dynamic sharing for the **route-cntrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mode dad-proxy

To enable duplicate address detection (DAD) proxy mode for IPv6 Neighbor Discovery (ND) suppress, use the **mode dad-proxy** command in ND suppress policy configuration mode. To disable this feature, use the **no** form of this command.

mode dad-proxy

Syntax Description

This command has no arguments or keywords.

Command Default

All multicast neighbor solicitation (NS) messages are suppressed.

Command Modes

ND suppress policy configuration mode (config-nd-suppress)

Command History

Release	Modification
15.1(2)SG	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The IPv6 Dad proxy feature responds on behalf of the address's owner when an address is already in use. Use the **mode dad-proxy** command to enable IPv6 DAD proxy when using IPv6 ND suppress. If your device does not support IPv6 multicast suppress, you can enable IPv6 DAD proxy by entering the **ipv6 nd dad-proxy** command in global configuration mode.

Examples

```
Device(config)# ipv6 nd suppress policy policy1
Device(config-nd-suppress)# mode dad-proxy
```

Related Commands

Command	Description
ipv6 nd dad-proxy	Enables the IPv6 ND DAD proxy feature on the device.
ipv6 nd suppress policy	Enables IPv6 ND multicast suppress and enters ND suppress policy configuration mode.

monitor event ipv6 static

To monitor the operation of the IPv6 static and IPv6 static Bidirectional Forwarding Detection for IPv6 (BFDv6) neighbors using event trace, use the **monitor event ipv6 static** command in privileged EXEC mode. To disable monitoring, use the **no** form of the command.

monitor event ipv6 static

no monitor event ipv6 static

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 static and IPv6 static BFD neighbors are not monitored.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1.0	This command was introduced.
15.1(2)T	This command was modified. It was integrated into Cisco IOS Release 15.1(2)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **monitor event ipv6 static** command to monitor the operation of IPv6 static and IPv6 static BFDv6 neighbors and collect data.

Examples

The following example enables event trace to monitor BFDv6 operation:

```
Router# monitor event ipv6 static
```

Related Commands

Command	Description
debug ipv6 static	Enables BFDv6 debugging.
show ipv6 static	Displays the current contents of the IPv6 routing table.

monitor event-trace cef ipv6 (global)

To configure event tracing for Cisco Express Forwarding IPv6 events, use the **monitor event-trace cef ipv6**command in global configuration mode. To disable event tracing for Cisco Express Forwarding, use the **no** form of this command.

monitor event-trace cef ipv6 {**disable**| **distribution**| **dump-file** *dump-file-name*| **enable**| **math** {**global**| *ipv6-address/n*}| **size** *number*| **stacktrace** [*depth*]| **vrf** *vrf-name* [**distribution**| **match**{**global**| *ipv6-address/n*}]}

no monitor event-trace cef ipv6 {**disable**| **distribution**| **dump-file** *dump-file-name*| **enable**| **match**| **size**| **stacktrace** [*depth*]| **vrf**}

Syntax Description

disable	Turns off event tracing for Cisco Express Forwarding IPv6 events.
distribution	Logs events related to the distribution of Cisco Express Forwarding Forwarding Information Base (FIB) tables to the line cards.
dump-file *dump-file-name*	Specifies the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.
enable	Turns on event tracing for Cisco Express Forwarding IPv6 events if it had been enabled with the **monitor event-trace cef ipv6**command.
match	Turns on event tracing for Cisco Express Forwarding IPv6 that matches global events or events that match a specific network address.
global	Specifies global events.
ipv6-address / *n*	Specifies an IPv6 address. This address must be in the form documented in RFC 2373: the address is specified in hexadecimals using 16-bit values between colons. The slash followed by a number (/ *n*) indicates the number of bits that do not change. Range: 0 to 128.

size *number*	Sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536. **Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace cef parameters** command. When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
stacktrace	Enables the stack trace at tracepoints.
depth	(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.
vrf *vrf-name*	Turns on event tracing for a Cisco Express Forwarding IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) table. The *vrf-name* argument specifies the name of the VRF.

Command Default

Event tracing for Cisco Express Forwarding IPv6 events is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **monitor event-trace cef ipv6**command to enable or disable event tracing for Cisco Express Forwarding IPv6 events.

The Cisco IOS software allows Cisco Express Forwarding to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value in one of two ways: using the **monitor event-trace cef ipv6**command in privileged EXEC mode or using the **monitor event-trace cef ipv6**command in global configuration mode.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace cef ipv6**command for each instance of a trace.

To determine whether event tracing is enabled by default for Cisco Express Forwarding IPv6 events, use the **show monitor event-trace cef ipv6**command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

Examples

The following example shows how to enable event tracing for Cisco Express Forwarding IPv6 events and configure the buffer size to 10000 messages.

```
Router(config)# monitor event-trace cef ipv6 enable
Router(config)# monitor event-trace cef ipv6 size 10000
```

Related Commands

Command	Description
monitor event-trace cef (EXEC)	Monitors and controls the event trace function for Cisco Express Forwarding.
monitor event-trace cef (global)	Configures event tracing for Cisco Express Forwarding.
monitor event-trace cef ipv4 (global)	Configures event tracing for Cisco Express Forwarding IPv4 events.
show monitor event-trace cef	Displays event trace messages for Cisco Express Forwarding.
show monitor event-trace cef events	Displays event trace messages for Cisco Express Forwarding events.
show monitor event-trace cef interface	Displays event trace messages for Cisco Express Forwarding interface events.
show monitor event-trace cef ipv4	Displays event trace messages for Cisco Express Forwarding IPv4 events.
show monitor event-trace cef ipv6	Displays event trace messages for Cisco Express Forwarding IPv6 events.

monitor event-trace ipv6 spd

To monitor Selective Packet Discard (SPD) state transition events, use the monitor event-trace ipv6 spd command in privileged EXEC mode. To disable this function, use the **no** form of this command.

monitor event-trace ipv6 spd

no monitor event-trace ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **monitor event-trace ipv6 spd** command to check SPD state transition events.

multi-topology

To enable multitopology Intermediate System-to-Intermediate System (IS-IS) for IPv6, use the **m ulti-topology** command in address family configuration mode. To disable multitopology IS-IS for IPv6, use the **no** form of this command.

multi-topology [transition]

no multi-topology

Syntax Description

transition	(Optional) Allows an IS-IS IPv6 user to continue to use single shortest path first (SPF) mode while upgrading to multitopology IS-IS for IPv6.

Command Default

Multitopology IS-IS is disabled by default.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

By default, the router runs IS-IS IPv6 in single SPF mode. The **multi-topology** command enables multitopology IS-IS for IPv6.

The optional transition keyword can be used to migrate from IS-IS IPv6 single SPF mode to multitopology IS-IS IPv6. When transition mode is enabled, the router advertises both multitopology type, length, and value (TLV) objects and single-SPF-mode IS-IS IPv6 TLVs, but the SPF is computed using the single-SPF-mode IS-IS IPv6 TLV. This action has the side effect of increasing the link-state packet (LSP) size.

Examples

The following example enables multitopology IS-IS for IPv6:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# multi-topology
```