

IPv6 Commands: ro to show bgp la

- router ospfv3, on page 2
- router-id (IPv6), on page 3
- router-id (OSPFv3), on page 5
- router-preference maximum, on page 7
- sec-level minimum, on page 9
- server name (IPv6 TACACS+), on page 10
- set ipv6 default next-hop, on page 11
- set ipv6 next-hop (BGP), on page 14
- set ipv6 next-hop (PBR), on page 17
- set ipv6 precedence, on page 19
- show bgp ipv6, on page 21
- show bgp ipv6 community, on page 25
- show bgp ipv6 community-list, on page 29
- show bgp ipv6 dampened-paths, on page 32
- show bgp ipv6 filter-list, on page 35
- show bgp ipv6 flap-statistics, on page 38
- show bgp ipv6 inconsistent-as, on page 41
- show bgp ipv6 labels, on page 44

router ospfv3

To enter Open Shortest Path First version 3 (OSPFv3) router configuration mode, use the router ospfv3 command in interface configuration mode.

router ospfv3 [*process-id*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.

Command Default

No OSPFv3 routing process is defined.

Command Modes

Global configuration (config)

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

Use the **router ospfv3** command to enter the OSPFv3 router configuration mode. From this mode, you can enter address-family configuration mode for IPv6 or IPv4 and then configure the IPv6 or IPv4 AF.

Examples

The following example enters OSPFv3 router configuration mode:

```
Router(config)# router ospfv3 1
Router(config-router)#
```

Related Commands

Command	Description
ipv6 ospf area	Enables OSPFv3 on an interface
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

router-id (IPv6)

To use a fixed router ID, use the **router-id** command in router configuration mode. To force Open Shortest Path First (OSPF) for IPv6 to use the previous OSPF for IPv6 router ID behavior, use the **no** form of this command.

router-id *router-id*
no router-id *router-id*

Syntax Description

router-id	Router ID for this OSPF process.

Command Default

The router ID is chosen automatically.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
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

- We recommend that you configure a Router ID using the **router-id** command in the OSPFv3 router configuration mode. A Router ID can be any 32-bit value in IP address format and is not restricted to the IPv4 addresses assigned to interfaces on the router. This Router ID should not be a routable IPv4 address.
- If you do not configure the Router ID and an IPv4 address exists, the OSPFv3 process selects the available IPv4 address as the Router ID
- If you have not configured a Router ID nor any IPv4 addresses, the OSPFv3 process cannot obtain a Router ID and the router displays this error message:

```
Error message - %OSPFv3 10 address-family ipv4 not running, please configure a router-id
```

- If multiple IPv4 addresses are available, a Router ID is selected using the same rules it applies for OSPFv2.
- If you use the **router-id** command on an OSPFv3 router process that is already active and has neighbors, the new Router ID takes effect immediately.

Examples

The following example specifies a fixed router ID:

```
Router(config-rtr)# router-id 10.1.1.1
```

Related Commands

Command	Description
clear ipv6 ospf	Clears the OSPF for IPv6 state based on the OSPF routing process ID.
ipv6 router eigrp	Configures the EIGRP IPv6 routing process.
ipv6 router ospf	Enables OSPF for IPv6 router configuration mode.

router-id (OSPFv3)

To use a fixed router ID, use the **router-id** command in Open Shortest Path First version 3 (OSPFv3) router configuration mode. To force OSPFv3 to use the previous OSPFv3 router ID behavior in IPv4, use the **no** form of this command.

router-id *router-id*
no router-id *router-id*

Syntax Description

router-id	Router ID for this OSPFv3 process.

Command Default

The router ID is chosen automatically.

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.

Usage Guidelines

- We recommend that you configure a Router ID using the **router-id** command in the OSPFv3 router configuration mode. A Router ID can be any 32-bit value in IP address format and is not restricted to the IPv4 addresses assigned to interfaces on the router. This Router ID should not be a routable IPv4 address.
- If you do not configure the Router ID and an IPv4 address exists, the OSPFv3 process selects the available IPv4 address as the Router ID
- If you have not configured a Router ID nor any IPv4 addresses, the OSPFv3 process cannot obtain a Router ID and the router displays this error message:

  ```
  Error message - %OSPFv3 10 address-family ipv4 not running, please configure a router-id
  ```

- If multiple IPv4 addresses are available, a Router ID is selected using the same rules it applies for OSPFv2.
- If you use the **router-id** command on an OSPFv3 router process that is already active and has neighbors, the new Router ID takes effect immediately.

Examples

This example specifies a fixed router ID:

```
Router(config-router)# router-id 10.1.1.1
```

Related Commands

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

router-preference maximum

To verify the advertised default router preference parameter value, use the **router-preference maximum** command in RA guard policy configuration mode.

router-preference maximum {**high** | **low** | **medium**}

Syntax Description

high	Default router preference parameter value is higher than the specified limit.
medium	Default router preference parameter value is equal to the specified limit.
low	Default router preference parameter value is lower than the specified limit.

Command Default

The router preference maximum value is not configured.

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 **router-preference maximum** command enables verification that the advertised default router preference parameter value is lower than or equal to a specified limit. You can use this command to give a lower priority to default routers advertised on trunk ports, and to give precedence to default routers advertised on access ports.

The **router-preference maximum** command limit are high, medium, or low. If, for example, this value is set to **medium** and the advertised default router preference is set to **high** in the received packet, then the packet is dropped. If the command option is set to **medium** or **low** in the received packet, then the packet is not dropped.

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 configures router-preference maximum verification to be high:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# router-preference maximum high
```

Related Commands

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

sec-level minimum

To specify the minimum security level parameter value when Cryptographically Generated Address (CGA) options are used, use the **sec-level minimum** command in Neighbor Discovery (ND) inspection policy configuration mode. To disable this function, use the **no** form of this command.

sec-level minimum *value*
no sec-level minimum *value*

Syntax Description

value	Minimum security level, which is a value from 1 to 7. The default security level is 1. The most secure level is 3.

Command Default

The default security level is 1.

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.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **sec-level minimum** command specifies the minimum security level parameter value when CGA options are used. Use the **sec-level minimum** command after enabling ND inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and specifies 2 as the minimum CGA security level:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# sec-level minimum 2
```

Related Commands

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

server name (IPv6 TACACS+)

To specify an IPv6 TACACS+ server, use the **server name**command in TACACS+ group server configuration mode. To remove the IPv6 TACACS+ server from configuration, use the **no** form of this command.

server name *server-name*
no server name *server-name*

Syntax Description

server-name	The IPv6 TACACS+ server to be used.

Command Default

No server name is specified.

Command Modes

TACACS+ group server configuration (config-sg-tacacs+)

Command History

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

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server name** command to specify an IPv6 TACACS+ server.

Examples

The following example shows how to specify an IPv6 TACACS+ server named server1:

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

Related Commands

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

set ipv6 default next-hop

To specify an IPv6 default next hop to which matching packets are forwarded, use the **set ipv6 default next-hop** command in route-map configuration mode. To delete the default next hop, use the **no** form of this command.

set ipv6 default [**vrf** *vrf-name* | **global**] **next-hop** *global-ipv6-address* [*global-ipv6-address...*]
no set ipv6 default [**vrf** *vrf-name* | **global**] **next-hop** *global-ipv6-address* [*global-ipv6-address...*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies explicitly that the default next-hops are under the specific Virtual Routing and Forwarding (VRF) instance.
global	(Optional) Specifies explicitly that the default next-hops are under the global routing table.
global-ipv6-address	IPv6 global address of the next hop to which packets are output. The next-hop router must be an adjacent router. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

Packets are not forwarded to a default next hop.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It 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.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *global-ipv6-address* argument.

Use the **set ipv6 default next-hop** command in policy-based routing PBR for IPv6 to specify an IPv6 next-hop address to which a packet is policy routed when the router has no route in the IPv6 routing table or the packets match the default route. The IPv6 next-hop address must be adjacent to the router; that is, reachable by using a directly connected IPv6 route in the IPv6 routing table. The IPv6 next-hop address also must be a global IPv6 address. An IPv6 link-local address cannot be used because the use of an IPv6 link-local address requires interface context.

If the software has no explicit route for the destination in the packet, then the software routes the packet to the next hop as specified by the **set ipv6 default next-hop** command. The optional specified IPv6 addresses are tried in turn.

Use the **ipv6 policy route-map** command, the **route-map** command, and the **match** and **set route-map** commands to define the conditions for PBR packets. The **ipv6 policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria, which are the conditions under which PBR occurs. The **set** commands specify the set actions, which are the particular routing actions to perform if the criteria enforced by the match commands are met.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**



Note The **set ipv6 next-hop** and **set ipv6 default next-hop** are similar commands. The **set ipv6 next-hop** command is used to policy route packets for which the router has a route in the IPv6 routing table. The **set ipv6 default next-hop** command is used to policy route packets for which the router does not have a route in the IPv6 routing table (or the packets match the default route).

Examples

The following example shows how to set the next hop to which the packet is routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:DB8:4:1::1/64 any
route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 default next-hop 2001:DB8:4:4::1/64
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 policy-based routing (PBR) on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.

Command	Description
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ipv6 next-hop (BGP)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy routing, use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop {*ipv6-address* [*link-local-address*] | **encapsulate l3vpn** *profile name* | **peer-address**}
no set ipv6 next-hop {*ipv6-address* [*link-local-address*] | **encapsulate l3vpn** *profile name* | **peer-address**}

Syntax Description

ipv6-address	IPv6 global address of the next hop to which packets are output. It need not be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
link-local-address	(Optional) IPv6 link-local address of the next hop to which packets are output. It must be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
encapsulate l3vpn	Sets the encapsulation profile for VPN nexthop.
profile name	Name of the Layer 3 encapsulation profile.
peer-address	(Optional) Sets the next hop to be the BGP peering address.

Command Default

IPv6 packets are forwarded to the next hop router in the routing table.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.2(4)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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SRE	This command was modified. The **encapsulate l3vpn** keyword was added.

Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific.

The **set** commands specify the *set actions* --the particular routing actions to perform if the criteria enforced by the **match** commands are met.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ipv6 next-hop** command has finer granularity than the per-neighbor **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**

Configuring the **set ipv6 next-hop** *ipv6-address* command on a VRF interface allows the next hop to be looked up in a specified VRF address family. In this context, the *ipv6-address* argument matches that of the specified VRF instance.

Examples

The following example configures the IPv6 multiprotocol BGP peer FE80::250:BFF:FE0E:A471 and sets the route map named nh6 to include the IPv6 next hop global addresses of Fast Ethernet interface 0 of the neighbor in BGP updates. The IPv6 next hop link-local address can be sent to the neighbor by the nh6 route map or from the interface specified by the **neighbor update-source** router configuration command.

```
router bgp 170
 neighbor FE80::250:BFF:FE0E:A471 remote-as 150
 neighbor FE80::250:BFF:FE0E:A471 update-source fastether 0
address-family ipv6
  neighbor FE80::250:BFF:FE0E:A471 activate
  neighbor FE80::250:BFF:FE0E:A471 route-map nh6 out
route-map nh6
 set ipv6 next-hop 3FFE:506::1
```



Note If you specify only the global IPv6 next hop address (the *ipv6-address* argument) with the **set ipv6 next-hop** command after specifying the neighbor interface (the *interface-type* argument) with the **neighbor update-source** command, the link-local address of the neighbor interface is included as the next hop in the BGP updates. Therefore, only one route map that sets the global IPv6 next hop address in BGP updates is required for multiple BGP peers that use link-local addresses.

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.

Command	Description
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 ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.
neighbor next-hop-self	Disables next-hop processing of BGP updates on the router.
neighbor update-source	Specifies that the Cisco IOS software allow BGP sessions to use any operational interface for TCP connections
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set ipv6 next-hop (PBR)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy-based routing (PBR), use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop {*next-hop-ipv6-address* [*next-hop-ipv6-address...*] | **encapsulate l3vpn** *encapsulation-profile* | **peer-address** | **recursive** *next-hop-ipv6-address* | **verify-availability** *next-hop-ipv6-address sequence* **track** *object-number*}
no set ipv6 next-hop {*next-hop-ipv6-address* [*next-hop-ipv6-address...*] | **encapsulate l3vpn** *encapsulation-profile* | **peer-address** | **recursive** *next-hop-ipv6-address* | **verify-availability** *next-hop-ipv6-address sequence* **track** *object-number*}

Syntax Description

next-hop-ipv6-address [*next-hop-ipv6-address ...*]	IPv6 global address of the next hop to which packets are sent. The next-hop router must be an adjacent router. The IPv6 address must be specified in hexadecimal using 16-bit values between colons as specified in RFC 2373.
encapsulate	Specifies the encapsulation profile for the next-hop VPN.
l3vpn	Specifies Layer 3 VPN encapsulation.
encapsulation-profile	Encapsulation profile name.
peer-address	Specifies the peer address. This keyword is specific to Border Gateway Protocol (BGP).
recursive *next-hop-ipv6-address*	Specifies the IPv6 address of the recursive next-hop router. • The next-hop IPv6 address must be assigned separately from the recursive next-hop IPv6 address.
verify-availability	Verifies if the next-hop router is reachable.
sequence	Sequence number to insert into the next-hop list. Valid values for the *sequence* argument are from 1 to 65535.
track *object-number*	Sets the next-hop router depending on the state of a tracked object number. Valid values for the *object-number* argument are from 1 to 1000.

Command Default

Packets are not forwarded to a default next hop.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.

Release	Modification
12.2(33)SXI4	This command was integrated into 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.
15.4(2)S	This command was modified. The **recursive** keyword was added.

Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *next-hop-ipv6-address* argument. You must specify an IPv6 address; an IPv6 link-local address cannot be used because the use of an IPv6 link-local address requires interface context.

The *next-hop-ipv6-address* argument must specify an address that is configured in the IPv6 Routing Information Base (RIB) and is directly connected. A directly connected address is covered by an IPv6 prefix configured on an interface, or an address covered by an IPv6 prefix specified on a directly connected static route.

Examples

The following example shows how to set the next hop to which packets are routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:DB8::1 any
!
route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 next-hop 2001:DB8::F
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets are forwarded.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ipv6 precedence

To set the precedence value in the IPv6 packet header, use the **set ipv6 precedence** command in route-map configuration mode. To remove the precedence value, use the **no** form of this command.

set ipv6 precedence *precedence-value*
no set ipv6 precedence *precedence-value*

Syntax Description

precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into 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.

Usage Guidelines

The way the network gives priority (or some type of expedited handling) to the marked traffic is through the application of weighted fair queueing (WFQ) or weighted random early detection (WRED) at points downstream in the network. Typically, you would set IPv6 precedence at the edge of the network (or administrative domain) and have queueing act on it thereafter. WFQ can speed up handling for high precedence traffic at congestion points. WRED ensures that high precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from keywords such as routine and priority to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of Cisco high-end Internet quality of service (QoS), IPv6 precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network. For example, IPv6 precedence 2 can be given 90 percent of the bandwidth on output links in the network, and IPv6 precedence 6 can be given 5 percent using the distributed weight fair queueing (DWFQ) implementation on the Versatile Interface Processors (VIPs).

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

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

Examples

The following example sets the IPv6 precedence value to 5 for packets that pass the route map match:

```
interface serial 0
 ipv6 policy route-map texas
!
route-map cisco1
 match length 68 128
 set ipv6 precedence 5
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of 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	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.

show bgp ipv6

To display entries in the IPv6 Border Gateway Protocol (BGP) routing table, use the **show bgp ipv6**command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} [*ipv6-prefix/prefix-length*] [**longer-prefixes**] [**labels**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-prefix	(Optional) IPv6 network number, entered to display a particular network in the IPv6 BGP routing table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays the route and more specific routes.
labels	(Optional) Displays Multiprotocol Label Switching (MPLS) label information.

Command Modes

User EXEC
Privileged EXEC

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	MPLS label information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	MPLS label value advertised for the IPv6 prefix was added to the display.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.2(25)S	6PE multipath information was added to the display.
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.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **show bgp ipv6**command provides output similar to the **show ip bgp**command, except that it is IPv6-specific.

Examples

The following is sample output from the **show bgp ipv6**command:

```
Router# show bgp ipv6 unicast
BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*                   3FFE:C00:E:C::2                        0 3748 4697 1752 i
*                   3FFE:1100:0:CC00::1
                                                           0 1849 1273 1752 i
*  2001:618:3::/48  3FFE:C00:E:4::2          1             0 4554 1849 65002 i
*>                  3FFE:1100:0:CC00::1
                                                           0 1849 65002 i
*  2001:620::/35    2001:0DB8:0:F004::1
                                                           0 3320 1275 559 i
*                   3FFE:C00:E:9::2                        0 1251 1930 559 i
*                   3FFE:3600::A                           0 3462 10566 1930 559 i
*                   3FFE:700:20:1::11
                                                           0 293 1275 559 i
*                   3FFE:C00:E:4::2          1             0 4554 1849 1273 559 i
*                   3FFE:C00:E:B::2                        0 237 3748 1275 559 i
```

The table below describes the significant fields shown in the display.

Table 1: show bgp ipv6 Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp ipv6**command, showing information for prefix 3FFE:500::/24:

```
Router# show bgp ipv6 unicast 3FFE:500::/24
BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  Advertised to peer-groups:
     6BONE
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 673, flapped 429 times in 10:47:45
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 3938, flapped 596 times in 13:03:06, reuse in 00:59:10
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
```

The following is sample output from the **show bgp ipv6**command, showing MPLS label information for an IPv6 prefix that is configured to be an IPv6 edge router using MPLS:

```
Router# show bgp ipv6 unicast 2001:0DB8::/32
BGP routing table entry for 2001:0DB8::/32, version 15
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    ::FFFF:192.168.99.70 (metric 20) from 192.168.99.70 (192.168.99.70)
      Origin IGP, localpref 100, valid, internal, best, mpls label 17
```

To display the top of the stack label with label switching information, enter the **show bgp ipv6**EXEC command with the **labels** keyword:

```
Router# show bgp ipv6 unicast labels
Network              Next Hop              In tag/Out tag
2001:0DB8::/32       ::FFFF:192.168.99.70   notag/20
```

Note If a prefix has not been advertised to any peer, the display shows "Not advertised to any peer."

The following is sample output from the **show bgp ipv6**command, showing 6PE multipath information. The prefix 4004::/64 is received by BGP from two different peers and therefore two different paths:

```
Router# show bgp ipv6 unicast
BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 community

To display routes that belong to specified IPv6 Border Gateway Protocol (BGP) communities, use the **show bgp ipv6 community** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **community** [*community-number*] [**exact-match**] [**local-as** | **no-advertise** | **no-export**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
community-number	(Optional) Valid value is a community number in the range from 1 to 4294967295 or AA:NN (autonomous system-community number:2-byte number).
exact-match	(Optional) Displays only routes that have an exact match.
local-as	(Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
no-advertise	(Optional) Displays only routes that are not advertised to any peer (well-known community).
no-export	(Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).

Command Modes

User EXEC
Privileged EXEC

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.
12.3(2)T	The **unicast** and **exact-match** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** 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.

Usage Guidelines

The **show bgp ipv6 community** command provides output similar to the **show ip bgp community**command, except it is IPv6-specific.

Communities are set with the **set community** route-map configuration command. You must enter the numerical communities before the well-known communities. For example, the following string is not valid:

```
Router# show ipv6 bgp community local-as 111:12345
```

Use one of the following strings instead:

```
Router# show ipv6 bgp community 111:12345 local-as
Router# show ipv6 bgp unicast community 111:12345 local-as
```

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 community** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
       Network              Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64       ::                                       0 32768 i
*> 2001:0DB8:0:1:1::/80      ::                                       0 32768 ?
*> 2001:0DB8:0:2::/64        2001:0DB8:0:3::2                            0 2 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:3::2                            0 2 ?
* 2001:0DB8:0:3::1/64        2001:0DB8:0:3::2                            0 2 ?
*>                          ::                                       0 32768 ?
*> 2001:0DB8:0:4::/64        2001:0DB8:0:3::2                            0 2 ?
*> 2001:0DB8:0:5::1/64       ::                                       0 32768 ?
*> 2001:0DB8:0:6::/64        2000:0:0:3::2                            0 2 3 i
*> 2010::/64                 ::                                       0 32768 ?
*> 2020::/64                 ::                                       0 32768 ?
*> 2030::/64                 ::                                       0 32768 ?
*> 2040::/64                 ::                                       0 32768 ?
*> 2050::/64                 ::                                       0 32768 ?
```

The table below describes the significant fields shown in the display.

Table 2: show bgp ipv6 community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e--Entry originated from the Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
ip bgp-community new-format	Displays BGP communities in the format AA:NN (autonomous system-community number:2-byte number).

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 community-list

To display routes that are permitted by the IPv6 Border Gateway Protocol (BGP) community list, use the **show bgp ipv6 community-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **community-list** {*numbername*} [**exact-match**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
number	Community list number in the range from 1 to 199.
name	Community list name.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC
Privileged EXEC

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.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast**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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 unicast community-list**and **show bgp ipv6 multicast community-list**commands provide output similar to the **show ip bgp community-list**command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output of the **show bgp ipv6 community-list** command for community list number 3:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast community-list 3
BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
    Network                Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64      2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:1:1::/80    2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:2::1/64     ::                                   0 32768 i
*> 2001:0DB8:0:2:1::/80    ::                                   0 32768 ?
* 2001:0DB8:0:3::2/64      2001:0DB8:0:3::1                         0 1 ?
*>                       ::                                   0 32768 ?
*> 2001:0DB8:0:4::2/64      ::                                   0 32768 ?
*> 2001:0DB8:0:5::/64       2001:0DB8:0:3::1                         0 1 ?
*> 2010::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2020::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2030::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2040::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2050::/64                2001:0DB8:0:3::1                         0 1 ?
```

The table below describes the significant fields shown in the display.

Table 3: show bgp ipv6 community-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 dampened-paths

To display IPv6 Border Gateway Protocol (BGP) dampened routes, use the **show bgp ipv6 dampened-paths** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {unicast | multicast} dampening dampened-paths

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
dampening	Displays detailed information about dampening.

Command Modes

User EXEC
Privileged EXEC

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.
12.3(2)T	The **unicast** and **dampening** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** 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.
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 **show bgp ipv6 dampened-paths**and **show bgp ipv6 unicast dampening dampened-paths**commands provide output similar to the **show ip bgp dampened-paths**command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 dampened-paths** command:



Note The command output is the same whether or not the **unicast, multicast,**and **dampening** keywords are used. The **unicast**and **dampening**keywords are available only in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast dampening dampened-paths
BGP table version is 12610, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From             Reuse    Path
*d 3FFE:1000::/24   3FFE:C00:E:B::2  00:00:10 237 2839 5609 i
*d 2001:228::/35    3FFE:C00:E:B::2  00:23:30 237 2839 5609 2713 i
```

The table below describes the significant fields shown in the display.

Table 4: show bgp ipv6 dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e--Entry originated from the Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP.
Network	Indicates the network to which the route is dampened.
From	IPv6 address of the peer that advertised this path.

Field	Description
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp ipv6 dampening	Clears IPv6 BGP route dampening information and unsuppresses the suppressed routes.

show bgp ipv6 filter-list

To display routes that conform to a specified IPv6 filter list, use the **show bgp ipv6 filter-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **filter-list** *access-list-number*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
access-list-number	Number of an IPv6 autonomous system path access list. It can be a number from 1 to 199.

Command Modes

User EXEC
Privileged EXEC

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.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast**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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 filter-list**command provides output similar to the **show ip bgp filter-list**command, except that it is IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 filter-list** command for IPv6 autonomous system path access list number 1:



Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast filter-list 1
BGP table version is 26, local router ID is 192.168.0.2
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
    Network              Next Hop                            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64        2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:1:1::/80      2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:3::/64        2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:4::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:5::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 1 ?
*> 2001:0DB8:0:6::1/64       ::                                         32768  i
*> 2030::/64                 2001:0DB8:0:4::2                         0 1
*> 2040::/64                 2001:0DB8:0:4::2                         0 2 1 ?
*> 2050::/64                 2001:0DB8:0:4::2                         0 2 1 ?
```

The table below describes the significant fields shown in the display.

Table 5: show bgp ipv6 filter-list Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented any time the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. It can be one of the following values: • i--The entry was originated with the IGP and advertised with a **network** router configuration command. • e--The route originated with EGP. • ?--The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

Related Commands

Command	Description
ip as-path access-list	Defines a BGP autonomous system path access list.

show bgp ipv6 flap-statistics

To display IPv6 Border Gateway Protocol (BGP) flap statistics , use the **show bgp ipv6 flap-statistics** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **dampening flap-statistics** [**regexp** *regular-expression* | **quote-regexp** *regular-expression* | **filter-list** *list* | *ipv6-prefix/prefix-length* [**longer-prefix**]]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
dampening	Displays detailed information about dampening.
regexp *regular-expression*	(Optional) Displays flap statistics for all the paths that match the regular expression.
quote-regexp *regular-expression*	(Optional) Displays flap statistics for all the paths that match the regular expression as a quoted string of characters.
filter-list *list*	(Optional) Displays flap statistics for all the paths that pass the access list.
ipv6-prefix	(Optional) Displays flap statistics for a single entry at this IPv6 network number.
/*ipv6-prefix*	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value
longer-prefix	(Optional) Displays flap statistics for more specific entries.

Command Modes

User EXEC

Privileged EXEC

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.
12.3(2)T	The **unicast** and **dampening** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords were added.

Release	Modification
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 **show bgp ipv6 unicast dampening flap-statistics** and **show bgp ipv6 multicast dampening flap-statistics** commands provide output similar to the **show ip bgp flap-statistics** command, except they are IPv6-specific.

If no arguments or keywords are specified, the router displays flap statistics for all routes.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the**unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the**unicast** or**multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 flap-statistic s** command without arguments or keywords:

Note The output is the same whether or not the **unicast**, **multicast** and **dampening** keywords are used. The **unicast** and **dampening** keywords are available only in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast dampening flap-statistics

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From            Flaps Duration Reuse    Path
*d 2001:200::/35    3FFE:1100:0:CC00::1
                                    12145 10:09:15 00:57:10 1849 2914 4697 2500
*  2001:218::/35    2001:0DB8:0:F004::1
                                    2     00:03:44          3462 4697
```

The table below describes the significant fields shown in the display.

Table 6: show bgp ipv6 flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Route to the network indicated is dampened.
From	IPv6 address of the peer that advertised this path.
Flaps	Number of times the route has flapped.
Duration	Time (hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp ipv6 flap-statistics	Clears IPv6 BGP flap statistics.
ip as-path access-list	Defines a BGP autonomous system path access list.

show bgp ipv6 inconsistent-as

To display IPv6 Border Gateway Protocol (BGP) routes with inconsistent originating autonomous systems, use the **show bgp ipv6 inconsistent-as** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **inconsistent-as**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.

Command Modes

User EXEC
Privileged EXEC

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.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast**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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 unicast inconsistent-as**and **show bgp ipv6 multicast inconsistent-as**commands provide output similar to the **show ip bgp inconsistent-as** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 inconsistent-as** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast inconsistent-as
BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  3FFE:1300::/24   2001:0DB8:0:F004::1                    0 3320 293 6175 ?
*                   3FFE:C00:E:9::2                       0 1251 4270 10318 ?
*                   3FFE:3600::A                          0 3462 6175 ?
*                   3FFE:700:20:1::11                     0 293 6175 ?
```

The table below describes the significant fields shown in the display.

Table 7: show bgp ipv6 inconsistent-as Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.

Field	Description
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp ipv6 labels

To display the status of all IPv6 Border Gateway Protocol (BGP) connections, use the **show bgp ipv6 labels**command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **labels**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords were added.

Usage Guidelines

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 labels**command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast labels
Network                    Next Hop        In label/Out label
2001:1:101::1/128          ::FFFF:172.17.1.1  nolabel/19
2001:3:101::1/128          ::FFFF:172.25.8.8  nolabel/19
```

The table below describes the significant fields shown in the display.

Table 8: show bgp ipv6 labels Field Descriptions

Field	Description
Network	IPv6 address of the network the entry describes.

Field	Description
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
In label/Out label	IPv6 BGP connections.