IPv6 Commands: show ipv6 ri to si

show ipv6 rip

To display information about current IPv6 Routing Information Protocol (RIP) processes, use the **show ipv6 rip** command in user EXEC or privileged EXEC mode.

Cisco IOS XE Release 3.9S, Cisco IOS Release 15.3(2)S, and Later Releases

show ipv6 rip [*name*] [**vrf** *vrf-name*] [**database** | **next-hops**]

Releases Prior to Cisco IOS XE Release 3.9S and Cisco IOS Release 15.3(2)S

show ipv6 rip [*name*] [**database** | **next-hops**]

Syntax Description

name	(Optional) Name of the RIP process. If the name is not entered, details of all configured RIP processes are displayed.
vrf *vrf-name*	(Optional) Displays information about the specified Virtual Routing and Forwarding (VRF) instance.
database	(Optional) Displays information about entries in the specified RIP IPv6 routing table.
next-hops	(Optional) Displays information about the next hop addresses for the specified RIP IPv6 process. If no RIP process name is specified, the next-hop addresses for all RIP IPv6 processes are displayed.

Command Default   Information about all current IPv6 RIP processes is displayed.

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. The *name* argument and the **database** and **next-hops** keywords were added.

Release	Modification
12.2(13)T	The command was modified. The *name* argument, and the **database** and **next-hops** keywords were 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 implemented on Cisco 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.9S	This command was modified. The **vrf** *vrf-name* keyword/argument pair was added.
15.3(2)S	This command was integrated into Cisco IOS Release 15.3(2)S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

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

```
Device# show ipv6 rip

RIP process "one", port 521, multicast-group FF02::9, pid 55
     Administrative distance is 25. Maximum paths is 4
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 8883, trigger updates 2
  Interfaces:
    Ethernet2
  Redistribution:
RIP process "two", port 521, multicast-group FF02::9, pid 61
     Administrative distance is 120. Maximum paths is 4
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 8883, trigger updates 0
  Interfaces:
    None
  Redistribution:
```

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

Table 1: show ipv6 rip Field Descriptions

Field	Description
RIP process	The name of the RIP process.

Field	Description
port	The port that the RIP process is using.
multicast-group	The IPv6 multicast group of which the RIP process is a member.
pid	The process identification number (pid) assigned to the RIP process.
Administrative distance	Used to rank the preference of sources of routing information. Connected routes have an administrative distance of 1 and are preferred over the same route learned by a protocol with a larger administrative distance value.
Updates	The value (in seconds) of the update timer.
expire	The interval (in seconds) in which updates expire.
Holddown	The value (in seconds) of the hold-down timer.
garbage collect	The value (in seconds) of the garbage-collect timer.
Split horizon	The split horizon state is either on or off.
poison reverse	The poison reverse state is either on or off.
Default routes	The origination of a default route into RIP. Default routes are either generated or not generated.
Periodic updates	The number of RIP update packets sent on an update timer.
trigger updates	The number of RIP update packets sent as triggered updates.

The following is sample output from the **show ipv6 rip database** command.

```
Device# show ipv6 rip one database

RIP process "one", local RIB
 2001:72D:1000::/64, metric 2
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
 2001:72D:2000::/64, metric 2, installed
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
 2001:72D:3000::/64, metric 2, installed
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
     Ethernet1/2001:DB8::1, expires in 120 secs
 2001:72D:4000::/64, metric 16, expired, [advertise 119/hold 0]
     Ethernet2/2001:DB8:0:ABCD::1
 3004::/64, metric 2 tag 2A, installed
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
```

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

Table 2: show ipv6 rip database Field Descriptions

Field	Description
RIP process	The name of the RIP process.
2001:72D:1000::/64	The IPv6 route prefix.
metric	Metric for the route.
installed	Route is installed in the IPv6 routing table.
Ethernet2/2001:DB8:0:ABCD::1	Interface and LL next hop through which the IPv6 route was learned.
expires in	The interval (in seconds) before the route expires.
advertise	For an expired route, the value (in seconds) during which the route will be advertised as expired.
hold	The value (in seconds) of the hold-down timer.
tag	Route tag.

The following is sample output from the **show ipv6 rip next-hops** command.

```
Device# show ipv6 rip one next-hops

RIP process "one", Next Hops
  FE80::210:7BFF:FEC2:ACCF/Ethernet4/2 [1 routes]
  FE80::210:7BFF:FEC2:B286/Ethernet4/2 [2 routes]
```

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

Table 3: show ipv6 rip next-hops Field Descriptions

Field	Description
RIP process	The name of the RIP process.
2001:DB8:0:1::1/Ethernet4/2	The next-hop address and interface through which it was learned. Next hops are either the addresses of IPv6 RIP neighbors from which we have learned routes or explicit next hops received in IPv6 RIP advertisements.
	Note An IPv6 RIP neighbor may choose to advertise all its routes with an explicit next hop. In this case the address of the neighbor would not appear in the next hop display.

Field	Description
[1 routes]	The number of routes in the IPv6 RIP routing table using the specified next hop.

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

```
Device# show ipv6 rip vrf red

    RIP VRF "red", port 521, multicast-group 2001:DB8::/32, pid 295
    Administrative distance is 120. Maximum paths is 16
    Updates every 30 seconds, expire after 180
    Holddown lasts 0 seconds, garbage collect after 120
    Split horizon is on; poison reverse is off
    Default routes are not generated
    Periodic updates 99, trigger updates 3
    Full Advertisement 0, Delayed Events 0
 Interfaces:
   Ethernet0/1
   Loopback2
 Redistribution:
   None
```

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

Table 4: show ipv6 rip vrf Field Descriptions

Field	Description
RIP VRF	The name of the RIP VRF.
port	The port that the RIP process is using.
multicast-group	The IPv6 multicast group of which the RIP process is a member.
Administrative distance	Used to rank the preference of sources of routing information. Connected routes have an administrative distance of 1 and are preferred over the same route learned by a protocol with a larger administrative distance value.
Updates	The value (in seconds) of the update timer.
expires after	The interval (in seconds) in which updates expire.
Holddown	The value (in seconds) of the hold-down timer.
garbage collect	The value (in seconds) of the garbage-collect timer.
Split horizon	The split horizon state is either on or off.
poison reverse	The poison reverse state is either on or off.

Field	Description
Default routes	The origination of a default route into RIP. Default routes are either generated or not generated.
Periodic updates	The number of RIP update packets sent on an update timer.
trigger updates	The number of RIP update packets sent as triggered updates.

The following is sample output from **show ipv6 rip vrf next-hops** command:

```
Device# show ipv6 rip vrf blue next-hops

    RIP VRF "blue", local RIB
     AAAA::/64, metric 2, installed
    Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00, expires in 177 secs
```

Table 5: show ipv6 rip vrf next-hops Field Descriptions

Field	Description
RIP VRF	The name of the RIP VRF.
metric	Metric for the route.
installed	Route is installed in the IPv6 routing table.
Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00	The next hop address and interface through which it was learned. Next hops are either the addresses of IPv6 RIP neighbors from which we have learned routes, or explicit next hops received in IPv6 RIP advertisements. **Note** An IPv6 RIP neighbor may choose to advertise all its routes with an explicit next hop. In this case the address of the neighbor would not appear in the next hop display.
expires in	The interval (in seconds) before the route expires.

The following is sample output from **show ipv6 rip vrf database** command:

```
Device# show ipv6 rip vrf blue database

     RIP VRF "blue", Next Hops
    FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0 [1 paths]
```

Table 6: show ipv6 rip vrf database Field Descriptions

Field	Description
RIP VRF	The name of the RIP VRF.
FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0	Interface and LL next hop through which the IPv6 route was learned.
1 paths	Indicates the number of unique paths to this router that exist in the routing table.

Related Commands

Command	Description
clear ipv6 rip	Deletes routes from the IPv6 RIP routing table.
debug ipv6 rip	Displays the current contents of the IPv6 RIP routing table.
ipv6 rip vrf-mode enable	Enables VRF-aware support for IPv6 RIP.

show ipv6 route

To display contents of the IPv6 routing table, use the **show ipv6 route** command in user EXEC or privileged EXEC mode.

show ipv6 route [*ipv6-address*| *ipv6-prefix*/*prefix-length* [**longer-prefixes**]| [*protocol*] | [**repair**] | [**updated** [**boot-up**] [*day month*] [*time*]]| **interface** *type number*| **nd**| **nsf**| **table** *table-id* | **watch**]

Syntax Description

ipv6-address	(Optional) Displays routing information for a specific IPv6 address.
ipv6-prefix	(Optional) Displays routing information for a specific IPv6 network.
/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 output for longer prefix entries.
protocol	(Optional) The name of a routing protocol or the keyword **connected**, **local**, **mobile**, or **static**. If you specify a routing protocol, use one of the following keywords: **bgp**, **isis**, **eigrp**, **ospf**, or **rip**.
repair	(Optional) Displays routes with repair paths.
updated	(Optional) Displays routes with time stamps.
boot-up	(Optional) Displays routing information since bootup.
day month	(Optional) Displays routes since the specified day and month.
time	(Optional) Displays routes since the specified time, in *hh:mm* format.
interface	(Optional) Displays information about the interface.
type	(Optional) Interface type.
number	(Optional) Interface number.
nd	(Optional) Displays only routes from the IPv6 Routing Information Base (RIB) that are owned by Neighbor Discovery (ND).

nsf	(Optional) Displays routes in the nonstop forwarding (NSF) state.
repair	(Optional)
table table-id	(Optional) Displays IPv6 RIB table information for the specified table ID. The table ID must be in hexadecimal format. The range is from 0 to 0-0xFFFFFFFF.
watch	(Optional) Displays information about route watchers.

Command Default   If none of the optional syntax elements is chosen, all IPv6 routing information for all active routing tables is displayed.

Command Modes   User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was modified. The **isis** keyword was added, and the I1 - ISIS L1, I2 - ISIS L2, and IA - ISIS interarea fields were included in the command output.
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. The timer information was removed, and an indicator was added to display IPv6 Multiprotocol Label Switching (MPLS) interfaces.
12.2(13)T	This command was modified. The timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces.
12.2(14)S	This command was modified. The **longer-prefixes** 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.

Release	Modification
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **table**, **nsf**, **watch**, and **updated** keywords and the *day, month, table-id*, and *time* arguments were added.
15.2(2)S	This command was modified. The command output was enhanced to include route tag values in dotted-decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to include route tag values in dotted-decimal format.
15.1(1)SY	The **nd** keyword was added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, the longest match lookup is performed from the routing table, and only route information for that address or network is displayed. When a routing protocol is specified, only routes for that protocol are displayed. When the **connected**, **local**, **mobile**, or **static** keyword is specified, only the specified type of route is displayed. When the **interface** keyword and *type* and *number* arguments are specified, only routes for the specified interface are displayed.

Examples

The following is sample output from the **show ipv6 route** command when no keywords or arguments are specified:

```
Device# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   2001:DB8:4::2/48 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   2001:DB8:4::3/48 [0/0]
     via ::, Ethernet1/0
C   2001:DB8:4::4/48 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::5/48 [0/0]
     via ::, Loopback0
L   2001:DB8:4::6/48 [0/0]
     via ::, Serial6/0
C   2001:DB8:4::7/48 [0/0]
     via ::, Serial6/0
S   2001:DB8:4::8/48 [1/0]
     via 2001:DB8:1::1, Null
L   FE80::/10 [0/0]
     via ::, Null0
```

```
L   FF00::/8 [0/0]
     via ::, Null0
```
The table below describes the significant fields shown in the display.

Table 7: show ipv6 route Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • B—BGP derived • C—Connected • I1—ISIS L1—Integrated IS-IS Level 1 derived • I2—ISIS L2—Integrated IS-IS Level 2 derived • IA—ISIS interarea—Integrated IS-IS interarea derived • L—Local • R—RIP derived • S—Static
2001:DB8:4::2/48	Indicates the IPv6 prefix of the remote network.
[20/0]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via FE80::A8BB:CCFF:FE02:8B00	Specifies the address of the next device to the remote network.

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, only route information for that address or network is displayed. The following is sample output from the **show ipv6 route** command when IPv6 prefix 2001:DB8::/35 is specified. The fields in the display are self-explanatory.

```
Device# show ipv6 route 2001:DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

When you specify a protocol, only routes for that particular routing protocol are shown. The following is sample output from the **show ipv6 route bgp** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
```

```
B   2001:DB8:4::4/64 [20/0]
      via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

The following is sample output from the **show ipv6 route local** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L   2001:DB8:4::2/128 [0/0]
      via ::, Ethernet1/0
LC  2001:DB8:4::1/128 [0/0]
      via ::, Loopback0
L   2001:DB8:4::3/128 [0/0]
      via ::, Serial6/0
L   FE80::/10 [0/0]
      via ::, Null0
L   FF00::/8 [0/0]
      via ::, Null0
```

The following is sample output from the **show ipv6 route** command when the 6PE multipath feature is enabled. The fields in the display are self-explanatory.

```
Device# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
.
.
.
B   2001:DB8::/64 [200/0]
      via ::FFFF:172.16.0.1
      via ::FFFF:172.30.30.1
```

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show ipv6 route shortcut

To display the IPv6 routes that contain shortcuts, use the **show ipv6 route shortcut**command in privileged EXEC mode.

show ipv6 route shortcut

Syntax Description   This command has no arguments or keywords.

Command Default   IPv6 information about shortcuts for all active routing tables is displayed.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.

Usage Guidelines   The **show ipv6 route shortcut** command displays only the routes that have overriding shortcut paths.

Examples   The following is sample output from the **show ipv6 route shortcut**command:

```
Router# show ipv6 route shortcut
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - Neighbor Discovery, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S 7000:1::/64 [1/0]
    via 4000:1:1::1, Ethernet1/1 [Shortcut]
    via 5000:1:1::1, Ethernet1/1 [Shortcut]
    via Ethernet1/1, directly connected
S 8000:1:1::/64 [1/0]
    via 6000:1:1::1, Ethernet0/1 [Shortcut]
    via Ethernet0/0, directly connected
```
The table below describes the significant fields shown in the display.

Table 8: show ipv6 route shortcut Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • C--Connected • L--Local • S--Static • R--RIP derived • B--BGP derived • I1--ISIS L1--Integrated IS-IS Level 1 derived • I2--ISIS L2--Integrated IS-IS Level 2 derived • IA--ISIS interarea--Integrated IS-IS interarea derived
S 7000:1::/64 [1/0]	Indicates paths that may be shortcut paths.
via 4000:1:1::1, Ethernet1/1	Indicates a path that may be a shortcut path.
via 5000:1:1::1, Ethernet1/1 [Shortcut]	Indicates a path that may be a shortcut path.
via Ethernet1/1, directly connected	Shows routes connected to the router directly.

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show ipv6 route summary

To display the current contents of the IPv6 routing table in summary format, use the **show ipv6 route summary**command in user EXEC or privileged EXEC mode.

show ipv6 route summary

Syntax Description

This command has no arguments or keywords.

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.
12.2(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.

Examples

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

```
Router# show ipv6 route summary
IPv6 Routing Table Summary - 257 entries
  37 local, 35 connected, 25 static, 0 RIP, 160 BGP
  Number of prefixes:
    /16: 1, /24: 46, /28: 10, /32: 5, /35: 25, /40: 1, /48: 63, /64: 19
    /96: 15, /112: 1, /126: 31, /127: 4, /128: 36
```
The table below describes the significant fields shown in the display.

Table 9: show ipv6 route summary Field Descriptions

Field	Description
entries	Number of entries in the IPv6 routing table.

Field	Description
Route source	Number of routes that are present in the routing table for each route source, which can be local routes, connected routes, static routes, a routing protocol, prefix and address or name, and longer prefixes and address or name.
	Routing protocols can include RIP, IS-IS, OSPF, and BGP.
	Other route sources can be connected, local, static, or a specific interface.
Number of prefixes:	Number of routing table entries for given prefix length.

Related Commands

Command	Description
show ipv6 route	Displays the current contents of the IPv6 routing table.

show ipv6 route vrf

To display IPv6 routing table information associated with a VPN routing and forwarding (VRF) instance, use the **show ipv6 route vrf** command in user EXEC or privileged EXEC mode.

show ipv6 route vrf {*vrf-name*| *vrf-number*}[**tag** {*tag-value*| *tag-value-dotted-decimal* [*mask*]}]

Syntax Description

vrf-name	Name assigned to the VRF.
vrf-number	Hexadecimal number assigned to the VRF.
tag	(Optional) Displays information about route tags in the VRF table.
tag-value	(Optional) Displays route tag value in plain decimals.
tag-value-dotted-decimal	(Optional) Displays route tag values in dotted decimals.
mask	(Optional) Route tag wildcard mask.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
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.
15.2(2)S	This command was integrated into Cisco IOS Release 15.2(2)S. The **tag** keyword and the *tag-value*, *tag-value-dotted-decimal*, and *mask* arguments were added to enable the display of route tags as plain decimals or dotted decimals in the command output.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S. The **tag** keyword and the *tag-value*, *tag-value-dotted-decimal*, and *mask* arguments were added to enable the display of route tags as plain decimals or dotted decimals in the command output.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Release	Modification
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following sample output from the **show ipv6 route vrf** command displays information about the IPv6 routing table associated with VRF1:

```
Device# show ipv6 route vrf VRF1

IPv6 Routing Table VRF1 - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
C   2001:DB8:4::2/48 [0/0]
     via ::, FastEthernet0/0
L   2001:DB8:4::3/48 [0/0]
     via ::, FastEthernet0/0
B   2001:DB8:4::4/48 [200/0]
     via ::FFFF:192.168.1.4,
B   2001:DB8:4::5/48 [20/1]
     via 2001:8::1,
C   2001:DB8:4::6/48 [0/0]
     via ::, Loopback1
L   2001:DB8:4::7/48 [0/0]
     via ::, Loopback1
```

The following sample output from the **show ip route vrf** *vrf-name* **tag** command displays information about tagged IPv6 routes in vrf1:

```
Device# show ipv6 route vrf vrf1 tag 0.0.0.6

IPv6 Routing Table - vrf1 - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
Routing entry for 2001::/32
  Known via "static", distance 1, metric 0
  Tag 0.0.0.6
  Route count is 1/1, share count 0
  Routing paths:
    directly connected via Null0
      Last updated 00:00:23 ago
```

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

Table 10: show ipv6 route vrf Field Descriptions

Field	Description
Codes	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • I—IS-IS derived • L—Local • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route
via ::, FastEthernet0/0	Indicates how the route was derived.
Tag	Identifies the tag associated with the remote network.

show ipv6 routers

To display IPv6 router advertisement (RA) information received from on-link devices, use the **show ipv6 routers** command in user EXEC or privileged EXEC mode.

show ipv6 routers [*interface-type interface-number*] [**conflicts**] [**vrf vrf-name**] [**detail**]

Syntax Description

interface -type	(Optional) Specifies the Interface type.
interface -number	(Optional) Specifies the Interface number.
conflicts	(Optional) Displays RAs that differ from the RAs configured for a specified interface.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
detail	(Optional) Provides detail about the eligibility of the neighbor for election as the default device.

Command Default

When an interface is not specified, on-link RA information is displayed for all interface types. (The term *onl-ink* refers to a locally reachable address on the link.)

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.
12.4(2)T	Command output was updated to show the state of the default router preference (DRP) preference value as advertised by other devices.
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.
15.0(2)SE	The **vrf** *vrf-name* keyword and argument pair and the **detail** keyword were added.

Usage Guidelines

Devices that advertise parameters that differ from the RA parameters configured for the interface on which the RAs are received are marked as conflicting.

Examples

The following is sample output from the **show ipv6 routers** command when entered without an IPv6 interface type and number:

```
Device# show ipv6 routers

Device FE80::83B3:60A4 on Tunnel5, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Device FE80::290:27FF:FE8C:B709 on Tunnel57, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

The following sample output shows a single neighboring device that is advertising a high default device preference and is indicating that it is functioning as a Mobile IPv6 home agent on this link.

```
Device# show ipv6 routers

IPV6 ND Routers (table: default)
  Device FE80::100 on Ethernet0/0, last update 0 min
  Hops 64, Lifetime 50 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  HomeAgentFlag=1, Preference=High
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 2001::100/64 onlink autoconfig
    Valid lifetime 2592000, preferred lifetime 604800
```

The following table describes the significant fields shown in the displays.

Table 11: show ipv6 routers Field Descriptions

Field	Description
Hops	The configured hop limit value for the RA.
Lifetime	The configured lifetime value for the RA. A value of 0 indicates that the device is not a default device. A value other than 0 indicates that the device is a default device.
AddrFlag	If the value is 0, the RA received from the device indicates that addresses are not configured using the stateful autoconfiguration mechanism. If the value is 1, the addresses are configured using this mechanism.

Field	Description
OtherFlag	If the value is 0, the RA received from the device indicates that information other than addresses is not obtained using the stateful autoconfiguration mechanism. If the value is 1, other information is obtained using this mechanism. (The value of OtherFlag can be 1 only if the value of AddrFlag is 1.)
MTU	The maximum transmission unit (MTU).
HomeAgentFlag=1	The value can be either 0 or 1. A value of 1 indicates that the device from which the RA was received is functioning as a mobile IPv6 home agent on this link, and a value of 0 indicates it is not functioning as a mobile IPv6 home agent on this link.
Preference=High	The DRP value, which can be high, medium, or low.
Retransmit time	The configured RetransTimer value. The time value to be used on this link for neighbor solicitation transmissions, which are used in address resolution and neighbor unreachability detection. A value of 0 means the time value is not specified by the advertising device.
Prefix	A prefix advertised by the device. Also indicates if on-link or autoconfig bits were set in the RA message.
Valid lifetime	The length of time (in seconds) relative to the time the advertisement is sent that the prefix is valid for the purpose of on-link determination. A value of -1 (all ones, 0xffffffff) represents infinity.
preferred lifetime	The length of time (in seconds) relative to the time the advertisements is sent that addresses generated from the prefix via address autoconfiguration remain valid. A value of -1 (all ones, 0xffffffff) represents infinity.

When the *interface-type* and *interface-number* arguments are specified, RA details about that specific interface are displayed. The following is sample output from the **show ipv6 routers** command when entered with an interface type and number:

```
Device# show ipv6 routers tunnel 5

Device FE80::83B3:60A4 on Tunnel5, last update 5 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
```

Entering the **conflicts** keyword with the **show ipv6 routers** command displays information for devices that are advertising parameters different from the parameters configured for the interface on which the advertisements are being received, as the following sample output shows:

```
Device# show ipv6 routers conflicts

Device FE80::203:FDFF:FE34:7039 on Ethernet1, last update 1 min, CONFLICT
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 2003::/64 onlink autoconfig
     Valid lifetime -1, preferred lifetime -1
Device FE80::201:42FF:FECA:A5C on Ethernet1, last update 0 min, CONFLICT
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 2001::/64 onlink autoconfig
     Valid lifetime -1, preferred lifetime -1
```

Use of the **detail** keyword provides information about the preference rank of the device, its eligibility for election as default device, and whether the device has been elected:

```
Device# show ipv6 routers detail

Device FE80::A8BB:CCFF:FE00:5B00 on Ethernet0/0, last update 0 min
 Rank 0x811 (elegible), Default Router
 Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0, MTU=1500
 HomeAgentFlag=0, Preference=Medium, trustlevel = 0
 Reachable time 0 (unspecified), Retransmit time 0 (unspecified)
 Prefix 2001::/64 onlink autoconfig
   Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 rpf

To check Reverse Path Forwarding (RPF) information for a given unicast host address and prefix, use the **show ipv6 rpf** command in user EXEC or privileged EXEC mode.

show ipv6 rpf {*source-vrf* [*access-list*]| **vrf** *receiver-vrf*{*source-vrf* [*access-list*]| **select**}}

Syntax Description

source-vrf	Name or address of the virtual routing and forwarding (VRF) on which lookups are to be performed.
receiver-vrf	Name or address of the VRF in which the lookups originate.
access-list	Name or address of access control list (ACL) to be applied to the group-based VRF selection policy.
vrf	Displays information about the VRF instance.
select	Displays group-to-VRF mapping information.

Command Modes   User EXEC Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *receiver-vrf* keyword and argument were added.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **show ipv6 rpf**command displays information about how IPv6 multicast routing performs Reverse Path Forwarding (RPF). Because the router can find RPF information from multiple routing tables (for example, unicast Routing Information Base [RIB], multiprotocol Border Gateway Protocol [BGP] routing table, or static mroutes), the **show ipv6 rpf**command to display the source from which the information is retrieved.

Examples

The following example displays RPF information for the unicast host with the IPv6 address of 2001::1:1:2:

```
Router# show ipv6 rpf 2001::1:1:2
RPF information for 2001::1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
  Metric preference:110
  Metric:30
```
The table below describes the significant fields shown in the display.

Table 12: show ipv6 rpf Field Descriptions

Field	Description
RPF information for 2001::1:1:2	Source address that this information concerns.
RPF interface:Ethernet3/2	For the given source, the interface from which the router expects to get packets.
RPF neighbor:FE80::40:1:3	For the given source, the neighbor from which the router expects to get packets.
RPF route/mask:20::/64	Route number and mask that matched against this source.
RPF type:Unicast	Routing table from which this route was obtained, either unicast, multiprotocol BGP, or static mroutes.
RPF recursion count	Indicates the number of times the route is recursively resolved.
Metric preference:110	The preference value used for selecting the unicast routing metric to the Route Processor (RP) announced by the designated forwarder (DF).
Metric:30	Unicast routing metric to the RP announced by the DF.

show ipv6 snooping capture-policy

To display message capture policies, use the **show ipv6 snooping capture-policy** command in user EXEC or privileged EXEC mode.

show ipv6 snooping capture-policy [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first-hop message types on the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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 **show ipv6 snooping capture-policy** command displays IPv6 first-hop message capture policies.

Examples

The following example shows **show ipv6 snooping capture-policy** command output on the Ethernet 0/0 interface, on which the IPv6 Neighbor Discovery Protocol (NDP) Inspection and Router Advertisement (RA) Guard features are configured:

```
Router# show ipv6 snooping capture-policy

Hardware policy registered on Et0/0
Protocol   Protocol value   Message   Value   Action   Feature
ICMP       58               RS        85      punt     RA Guard
                                               punt     ND Inspection
ICMP       58               RA        86      drop     RA guard
                                               punt     ND Inspection
ICMP       58               NS        87      punt     ND Inspection
ICMP       58               NA        88      punt     ND Inspection
ICMP       58               REDIR     89      drop     RA Guard
                                               punt     ND Inspection
```

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

Table 13: show ipv6 snooping capture-policy Field Descriptions

Field	Description
Hardware policy registered on Fa4/11	A hardware policy contains a programmatic access list (ACL), with a list of access control entries (ACEs).
Protocol	The protocol whose packets are being inspected.
Message	The type of message being inspected.
Action	Action to be taken on the packet.
Feature	The inspection feature for this information.

show ipv6 snooping counters

To display information about the packets counted by the interface counter, use the **show ipv6 snooping counters**command in user EXEC or privileged EXEC mode.

show ipv6 snooping counters {**interface** *type number*| **vlan** *vlan-id*}

Syntax Description

interface *type number*	Displays first-hop packets that match the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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 **show ipv6 snooping counters** command displays packets handled by the switch that are being counted in interface counters. The switch counts packets captured per interface and records whether the packet was received, sent, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.

Examples

The following examples shows information about packets counted on Fast Ethernet interface 4/12:

```
Router# show ipv6 snooping counters interface Fa4/12
Received messages on Fa4/12:
Protocol        Protocol message
ICMPv6          RS       RA       NS       NA       REDIR   CPS     CPA
                0        4256     0        0        0       0       0
Bridged messages from Fa4/12:
Protocol        Protocol message
ICMPv6          RS       RA       NS       NA       REDIR   CPS     CPA
                0        4240     0        0        0       0       0
Dropped messages on Fa4/12:
Feature/Message RS       RA       NS       NA       REDIR   CPS     CPA
RA guard        0        16       0        0        0       0       0
Dropped reasons on Fa4/12:
RA guard        16   RA drop - reason:RA/REDIR received on un-authorized port
```

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

Table 14: show ipv6 snooping counters Field Descriptions

Field	Description
Received messages on:	The messages received on an interface.
Protocol	The protocol for which messages are being counted.
Protocol message	The type of protocol messages being counted.
Bridged messages from:	Bridged messages from the interface.
Dropped messages on:	The messages dropped on the interface.
Feature/message	The feature that caused the drop, and the type and number of messages dropped.
RA drop - reason:	The reason that these messages were dropped.

show ipv6 snooping features

To display information about about snooping features configured on the router, use the **show ipv6 snooping features** command in user EXEC or privileged EXEC mode.

show ipv6 snooping features

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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.

Usage Guidelines

The **show ipv6 snooping features** command displays the first-hop features that are configured on the router.

Examples

The following example shows that both IPv6 NDP inspection and IPv6 RA guard are configured on the router:

```
Router# show ipv6 snooping features

Feature name    priority state
RA guard            100   READY
NDP inspection       20   READY
```
The table below describes the significant fields shown in the display.

Table 15: show ipv6 snooping features Field Descriptions

Field	Description
Feature name	The names of the IPv6 global policy features configured on the router.
priority	The priority of the specified feature.
state	The state of the specified feature.

show ipv6 snooping policies

To display information about the configured policies and the interfaces to which they are attached, use the **show ipv6 snooping policies** command in user EXEC or privileged EXEC mode.

show ipv6 snooping policies {**interface** *type number*| **vlan** *vlan-id*}

Syntax Description

interface *type number*	Displays policies that match the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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.

Usage Guidelines

The **show ipv6 snooping policies** command displays all policies that are configured and lists the interfaces to which they are attached.

Examples

The following example shows information about all policies configured:

```
Device# show ipv6 snooping policies

NDP inspection policies configured:
Policy      Interface    Vlan
------      ---------    ----
trusted      Et0/0        all
             Et1/0        all
untrusted    Et2/0        all
RA guard policies configured:
Policy      Interface    Vlan
------      ---------    ----
host         Et0/0        all
             Et1/0        all
router       Et2/0        all
```
The table below describes the significant fields shown in the display.

Table 16: show ipv6 snooping policies Field Descriptions

Field	Description
NDP inspection policies configured:	Description of the policies configured for a specific feature.
Policy	Whether the policy is trusted or untrusted.
Interface	The interface to which a policy is attached.

show ipv6 source-guard policy

To display the IPv6 source-guard policy configuration, use the **show ipv6 source-guard policy** command in user EXEC or privileged EXEC mode.

show ipv6 source-guard policy [*source-guard-policy*]

Syntax Description

source-guard-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco Release 15.3(1)S.

Usage Guidelines

The **show ipv6 source-guard policy** command displays the IPv6 source-guard policy configuration, as well as all the interfaces on which the policy is applied. The command also displays IPv6 prefix guard information if the IPv6 prefix guard feature is enabled on the device.

Examples

```
Device# show ipv6 source-guard policy policy1

Policy policy1 configuration:
data-glean
prefix-guard
address-guard

Policy policy1 is applied on the following targets:
Target          Type  Policy           Feature       Target range
Et0/0           PORT  policy1          source-guard  vlan all
vlan 100        VLAN  policy1          source-guard  vlan all
```

Related Commands

Command	Description
ipv6 source-guard attach-policy	Applies IPv6 source guard on an interface.
ipv6 source-guard policy	Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.

show ipv6 source-guard policy

show ipv6 spd

To display the IPv6 Selective Packet Discard (SPD) configuration, use the **show ipv6 spd**command in privileged EXEC mode.

show ipv6 spd

Syntax Description   This command has no arguments or keywords.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines   Use the **show ipv6 spd** command to display the SPD configuration, which may provide useful troubleshooting information.

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

```
Router# show ipv6 spd
Current mode: normal
Queue max threshold: 74, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0
```
The table below describes the significant fields shown in the display.

Table 17: show ipv6 spd Field Description

Field	Description
Current mode: normal	The current SPD state or mode.
Queue max threshold: 74	The process input queue maximum.

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the SPD process input queue.

show ipv6 static

To display the current contents of the IPv6 routing table, use the **show ipv6 static** command in user EXEC or privileged EXEC mode.

show ipv6 static [*ipv6-address*| *ipv6-prefix*/*prefix-length*] [**interface** *type number*| **recursive**] [**detail**]

Syntax Description

ipv6-address	(Optional) Provides routing information for a specific IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
ipv6-prefix	(Optional) Provides routing information for a specific IPv6 network. 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.
interface	(Optional) Name of an interface.
type	(Optional, but required if the **interface** keyword is used) Interface type. For a list of supported interface types, use the question mark (?) online help function.
number	(Optional, but required if the **interface** keyword is used) Interface number. For specific numbering syntax for supported interface types, use the question mark (?) online help function.
recursive	(Optional) Allows the display of recursive static routes only.

detail	(Optional) Specifies the following additional information:
	• For valid recursive routes, the output path set and maximum resolution depth.
	• For invalid recursive routes, the reason why the route is not valid.
	• For invalid direct or fully specified routes, the reason why the route is not valid.

Command Default   All IPv6 routing information for all active routing tables is displayed.

Command Modes   User EXEC Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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 2.1.0	This command was modified. It was integrated into Cisco IOS XE Release 2.1.0.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.

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

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. Only the information matching the criteria specified in the command syntax is displayed. For example, when the *type number* arguments are specified, only the specified interface-specific routes are displayed.

Examples

When no options specified in the command, those routes installed in the IPv6 Routing Information Base (RIB) are marked with an asterisk, as shown in the following example:

```
Router# show ipv6 static

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
  5000::/16, interface Ethernet3/0, distance 1
* 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```
The table below describes the significant fields shown in the display.

Table 18: show ipv6 static Field Descriptions

Field	Description
via nexthop	Specifies the address of the next router in the path to the remote network.
distance 1	Indicates the administrative distance to the specified route.

Examples

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, only information about static routes for that address or network is displayed. The following is sample output from the **show ipv6 route** command when entered with the IPv6 prefix 2001:200::/35:

```
Router# show ipv6 static 2001:200::/35

IPv6 Static routes
Code: * - installed in RIB
* 2001:200::/35, via nexthop 4000::1, distance 1
  2001:200::/35, via nexthop 9999::1, distance 1
* 2001:200::/35, interface Ethernet2/0, distance 1
```

Examples

When an interface is supplied, only those static routes with the specified interface as the outgoing interface are displayed. The **interface** keyword may be used with or without the IPv6 address and prefix specified in the command statement.

```
Router# show ipv6 static interface ethernet 3/0
```

IPv6 Static routes Code: * - installed in RIB 5000::/16, interface Ethernet3/0, distance 1

Examples

When the **recursive** keyword is specified, only recursive static routes are displayed:

```
Router# show ipv6 static recursive
```

IPv6 Static routes Code: * - installed in RIB * 4000::/16, via nexthop 2001:1::1, distance 1 * 5555::/16, via nexthop 4000::1, distance 1 5555::/16, via nexthop 9999::1, distance 1

Examples

When the **detail** keyword is specified, the following additional information is displayed:

- For valid recursive routes, the output path set and maximum resolution depth.

- For invalid recursive routes, the reason why the route is not valid.

- For invalid direct or fully specified routes, the reason why the route is not valid.

```
Router# show ipv6 static detail

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
    Resolves to 1 paths (max depth 1)
    via Ethernet1/0
  5000::/16, interface Ethernet3/0, distance 1
    Interface is down
* 5555::/16, via nexthop 4000::1, distance 1
    Resolves to 1 paths (max depth 2)
    via Ethernet1/0
  5555::/16, via nexthop 9999::1, distance 1
    Route does not fully resolve
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ip route	Displays the current state of the routing table.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show ipv6 traffic**command in user EXEC or privileged EXEC mode.

show ipv6 traffic [**interface** [*interface type number*]]

Syntax Description

interface	(Optional) All interfaces. IPv6 forwarding statistics for all interfaces on which IPv6 forwarding statistics are being kept will be displayed.
interface type number	(Optional) Specified interface. Interface statistics that have occurred since the statistics were last cleared on the specific interface are displayed.

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, and output fields were added.
12.2(13)T	The modification to add output fields was integrated into this release.
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.
12.2(33)SRC	The *interface* argument and **interface** keyword were added.
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 devices.

Release	Modification
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
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 **show ipv6 traffic**command provides output similar to the **show ip traffic**command, except that it is IPv6-specific.

Examples

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

```
Device# show ipv6 traffic
IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a device
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 unicast RPF drop, 0 suppressed RPF drop
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent
ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 device solicit, 0 device advert, 0 redirects
```

The following is sample output for the show ipv6 interface command without IPv6 CEF running:

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

The following is sample output for the show ipv6 interface command with IPv6 CEF running:

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
    CEF Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

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

Table 19: show ipv6 traffic Field Descriptions

Field	Description
source-routed	Number of source-routed packets.
truncated	Number of truncated packets.
format errors	Errors that can result from checks performed on header fields, the version number, and packet length.
not a device	Message sent when IPv6 unicast routing is not enabled.
0 unicast RPF drop, 0 suppressed RPF drop	Number of unicast and suppressed reverse path forwarding (RPF) drops.
failed	Number of failed fragment transmissions.
encapsulation failed	Failure that can result from an unresolved address or try-and-queue packet.
no route	Counted when the software discards a datagram it did not know how to route.

Field	Description
unreach	Unreachable messages received are as follows: • routing--Indicates no route to the destination. • admin--Indicates that communication with the destination is administratively prohibited. • neighbor--Indicates that the destination is beyond the scope of the source address. For example, the source may be a local site or the destination may not have a route back to the source. • address--Indicates that the address is unreachable. • port--Indicates that the port is unreachable.
Unicast RPF access-list MINI	Unicast RPF access-list in use.
Process Switching	Displays process RPF counts, such as verification and suppressed verification drops.
CEF Switching	Displays CEF switching counts, such as verification drops and suppressed verification drops.

show ipv6 tunnel

To display IPv6 tunnel information, use the **show ipv6 tunnel**command in user EXEC or privileged EXEC mode.

show ipv6 tunnel

Syntax Description

This command has no arguments or keywords.

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.

Command History

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

For each tunnel running IPv6, use the **show ipv6 tunnel** command to display the tunnel unit number, the name of the dynamic routing protocol used by the tunnel, the time of last input, the number of packets in the last input, and the description string as set by the **description** command.

Examples

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

```
Router# show ipv6 tunnel
Tun Route  LastInp  Packets
  0 RIPng   never        0
  1   -    00:00:13    55495
  2   -     never        0
  3   -    00:00:21    14755
  4   -     never        0
  5   -    00:00:00    15840
```

```
 6   -      never          0
 7   -     00:00:18     16008
 8   -      never          0
 9   -      never          0
10   -      never          0
11   -     00:00:03     94801
12   -      1d02h           2
13   -      never          0
14   -     00:00:08    312190
15   -      never          0
16   -      never          0
17   -      never          0
18   -     00:00:05   1034954
19   -      never          0
20   -     00:00:01   1171114
21   -      never          0
```

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

Table 20: show ipv6 tunnel Field Descriptions

Field	Description
Tun	Tunnel number.
Route	Indicates whether IPv6 RIP is enabled (RIPng) on this tunnel interface or is not enabled (-).
Last Inp	Time of last input into the tunnel.
Packets	Number of packets in this tunnel.
Description (not shown in sample output)	Description of the tunnel as entered in interface configuration mode.

show ipv6 virtual-reassembly

To display Virtual Fragment Reassembly (VFR) configuration and statistical information on a specific interface, use the **show ipv6 virtual-reassembly** command in privileged EXEC mode.

show ipv6 virtual-reassembly interface *interface-type*

Syntax Description

interface	interface-type	Specifies the interface for which information is requested.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

This command shows the configuration and statistical information of VFR on the given interface.

Examples

The following example shows a typical display produced by this command:

```
Router# show ipv6 virtual-reassembly
All enabled IPv6 interfaces...
GigabitEthernet0/0/0:
   IPv6 Virtual Fragment Reassembly (IPV6VFR) is ENABLED [in]
   IPv6 configured concurrent reassemblies (max-reassemblies): 64
   IPv6 configured fragments per reassembly (max-fragments): 16
   IPv6 configured reassembly timeout (timeout): 3 seconds
   IPv6 configured drop fragments: OFF

   IPv6 current reassembly count:0
   IPv6 current fragment count:0
   IPv6 total reassembly count:20
   IPv6 total reassembly timeout count:0
```

The display is self-explanatory; it corresponds to the values used when you entered the **ipv6 virtual-reassembly** command.

Related Commands

Command	Description
ipv6 virtual-reassembly	Enables VFR on an interface.

show ipv6 virtual-reassembly features

To display Virtual Fragment Reassembly (VFR) information on all interfaces or on a specified interface, use the **show ipv6 virtual-reassembly features** command in privileged EXEC mode.

show ipv6 virtual-reassembly features [**interface** *interface-type*]

Syntax Description

interface *interface-type*	(Optional) Specifies the interface for which information is requested.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

This command shows the configuration and statistical information of VFR on a specified interface or on all interfaces. Use the optional **interface** *interface-type* keyword and argument to specify an interface. If you enter the **show ipv6 virtual-reassembly features** command without the keyword and argument, information about all interfaces is displayed.

Examples

The following example displays information about all interfaces:

```
Router# show ipv6 virtual-reassembly features

GigabitEthernet0/0/0:
  IPV6 Virtual Fragment Reassembly (IPV6 VFR) Current Status is ENABLED [in]
  Features to use if IPV6 VFR is Enabled:CLI
GigabitEthernet0/0/0:
  IPV6 Virtual Fragment Reassembly (IPV6 VFR) Current Status is ENABLED [out]
  Features to use if IPV6 VFR is Enabled:CLI
```

The display is self-explanatory; it corresponds to the values used when you entered the **ipv6 virtual-reassembly** command.

Related Commands

Command	Description
ipv6 virtual-reassembly	Enables VFR on an interface.
show ipv6 virtual-reassembly	Displays VFR configuration and statistical information.

show ipv6 wccp

To display the IPv6 Web Cache Communication Protocol (WCCP) global configuration and statistics, use the **show ipv6 wccp** command in user EXEC or privileged EXEC mode.

show ipv6 wccp [[**all**] [**capabilities**] [**summary**] [**interfaces**[**cef**| **counts**| **detail**]][**vrf** *vrf-name*][{**web-cache**| *service-number*}[[**assignment**] [**clients**] [**counters**] [**detail**] [**service**] [**view**]]]]

Syntax Description

summary	(Optional) Displays a summary of WCCP services.
capabilities	(Optional) Displays WCCP platform capabilities information.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance associated with a service group to display.
service-number	(Optional) Identification number of the web cache service group being controlled by the cache. The number can be from 0 to 254. For web caches using Cisco cache engines, the reverse proxy service is indicated by a value of 99.
interfaces	(Optional) Displays WCCP redirect interfaces.
cef	(Optional) Displays Cisco Express Forwarding interface statistics, including the number of input, output, dynamic, static, and multicast services.
counts	(Optional) Displays WCCP interface count statistics, including the number of Cisco Express Forwarding and process-switched output and input packets redirected.
detail	(Optional) Displays WCCP interface configuration statistics, including the number of input, output, dynamic, static, and multicast services.
web-cache	(Optional) Displays statistics for the web cache service.
all	(Optional) Displays statistics for all known services.
assignment	(Optional) Displays service group assignment information.

service	(Optional) Displays detailed information about a service, including the service definition and all other per-service information.
clients	(Optional) Displays detailed information about the clients of a service, including all per-client information. No per-service information is displayed.
detail	(Optional) Displays detailed information about the clients of a service, including all per-client information. No per-service information is displayed. Assignment information is also displayed.
counters	(Optional) Displays traffic counters.

Command Modes   User EXEC (>)

Privileged EXEC (#)

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 the **clear ipv6 wccp** command to reset all WCCP counters.

Use the **show ipv6 wccp** *service-number* **detail** command to display information about the WCCP client timeout interval and the redirect assignment timeout interval if those intervals are not set to their default value of 10 seconds.

Use the **show ipv6 wccp summary** command to show the configured WCCP services and a summary of their current state.

Examples   This section contains examples and field descriptions for the following forms of this command:

- **show ipv6 wccp** *service-number* (service mode displayed)

- **show ipv6 wccp** *service-number* **detail**

- **show ipv6 wccp interfaces**

- **show ipv6 wccp web-cache**

- **show ipv6 wccp web-cache counters**

- **show ipv6 wccp web-cache detail**

- **show ipv6 wccp web-cache detail** (bypass counters displayed)

- **show ipv6 wccp web-cache service**

- **show ipv6 wccp summary**

Examples   The following is sample output from the **show ipv6 wccp** *service-number* command:

```
Router# show ipv6 wccp 61

Global WCCP information:
    Router information:
        Router Identifier:                 2001:DB8:100::1

    Service Identifier: 61
        Protocol Version:                  2.01
        Number of Service Group Clients:   2
        Number of Service Group Routers:   1
        Total Packets Redirected:          0
          Process:                         0
          CEF:                             0
        Service mode:                      Open
        Service Access-list:               -none-
        Total Packets Dropped Closed:      0
        Redirect access-list:              -none-
        Total Packets Denied Redirect:     0
        Total Packets Unassigned:          0
        Group access-list:                 -none-
        Total Messages Denied to Group:    0
        Total Authentication failures:     0
        Total GRE Bypassed Packets Received: 0
          Process:                         0
          CEF:                             0
```

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

Table 21: show ipv6 wccp service-number Field Descriptions

Field	Description
Router information	A list of routers detected by the current router.
Protocol Version	The version of WCCP being used by the router in the service group.
Service Identifier	Indicates which service is detailed.
Number of Service Group Clients	The number of clients that are visible to the router and other clients in the service group.
Number of Service Group Routers	The number of routers in the service group.
Total Packets s/w Redirected	Total number of packets redirected by the router.
Service mode	Identifies the WCCP service mode. Options are Open or Closed.
Service Access-list	A named extended IP access list that defines the packets that will match the service.

Field	Description
Total Packets Dropped Closed	Total number of packets that were dropped when WCCP is configured for closed services and an intermediary device is not available to process the service.
Redirect Access-list	The name or number of the access list that determines which packets will be redirected.
Total Packets Denied Redirect	Total number of packets that were not redirected because they did not match the access list.
Total Packets Unassigned	Number of packets that were not redirected because they were not assigned to any cache engine. Packets may not be assigned during initial discovery of cache engines or when a cache is dropped from a cluster.
Group Access-list	Indicates which cache engine is allowed to connect to the router.
Total Messages Denied to Group	Indicates the number of packets denied by the *group-list* access list.
Total Authentication failures	The number of instances where a password did not match.
Total Bypassed Packets Received	The number of packets that have been bypassed. Process and Cisco Express Forwarding are switching paths within Cisco IOS software.

Examples

The following example displays WCCP client information and WCCP router statistics that include the type of services:

```
Router# show ipv6 wccp 61 detail

WCCP Client information:
        WCCP Client ID:         2001:DB8:1::11
        Protocol Version:       2.01
        State:                  Usable
        Redirection:            L2
        Packet Return:          L2
        Assignment:             MASK
        Connect Time:           1w0d
        Redirected Packets:
          Process:              0
          CEF:                  0
        GRE Bypassed Packets:
          Process:              0
          CEF:                  0
        Mask Allotment:         32 of 64 (50.00%)
        Assigned masks/values:  1/32

        Mask   SrcAddr    DstAddr    SrcPort DstPort
        ----   -------    -------    ------- -------
```

```
0000: ::3          ::F          0x0000  0x0000

Value SrcAddr      DstAddr      SrcPort DstPort
----- -------      -------      ------- -------
0000: ::           ::           0x0000  0x0000
0001: ::           ::2          0x0000  0x0000
0002: ::           ::4          0x0000  0x0000
0003: ::           ::6          0x0000  0x0000
0004: ::           ::8          0x0000  0x0000
0005: ::           ::A          0x0000  0x0000
0006: ::           ::C          0x0000  0x0000
0007: ::           ::E          0x0000  0x0000
0008: ::1          ::           0x0000  0x0000
0009: ::1          ::2          0x0000  0x0000
0010: ::1          ::4          0x0000  0x0000
0011: ::1          ::6          0x0000  0x0000
0012: ::1          ::8          0x0000  0x0000
0013: ::1          ::A          0x0000  0x0000
0014: ::1          ::C          0x0000  0x0000
0015: ::1          ::E          0x0000  0x0000
0016: ::2          ::           0x0000  0x0000
0017: ::2          ::2          0x0000  0x0000
0018: ::2          ::4          0x0000  0x0000
0019: ::2          ::6          0x0000  0x0000
0020: ::2          ::8          0x0000  0x0000
0021: ::2          ::A          0x0000  0x0000
0022: ::2          ::C          0x0000  0x0000
0023: ::2          ::E          0x0000  0x0000
0024: ::3          ::           0x0000  0x0000
0025: ::3          ::2          0x0000  0x0000
0026: ::3          ::4          0x0000  0x0000
0027: ::3          ::6          0x0000  0x0000
0028: ::3          ::8          0x0000  0x0000
0029: ::3          ::A          0x0000  0x0000
0030: ::3          ::C          0x0000  0x0000
0031: ::3          ::E          0x0000  0x0000


WCCP Client ID:       2001:DB8:1::12
Protocol Version:     2.01
State:                Usable
Redirection:          L2
Packet Return:        L2
Assignment:           MASK
Connect Time:         1w0d
Redirected Packets:
  Process:            0
  CEF:                0
GRE Bypassed Packets:
  Process:            0
  CEF:                0
Mask Allotment:       32 of 64 (50.00%)
Assigned masks/values: 1/32

Mask  SrcAddr      DstAddr      SrcPort DstPort
----  -------      -------      ------- -------
0000: ::3          ::F          0x0000  0x0000

Value SrcAddr      DstAddr      SrcPort DstPort
----- -------      -------      ------- -------
0000: ::           ::1          0x0000  0x0000
0001: ::           ::3          0x0000  0x0000
0002: ::           ::5          0x0000  0x0000
0003: ::           ::7          0x0000  0x0000
0004: ::           ::9          0x0000  0x0000
0005: ::           ::B          0x0000  0x0000
0006: ::           ::D          0x0000  0x0000
0007: ::           ::F          0x0000  0x0000
0008: ::1          ::1          0x0000  0x0000
0009: ::1          ::3          0x0000  0x0000
0010: ::1          ::5          0x0000  0x0000
0011: ::1          ::7          0x0000  0x0000
0012: ::1          ::9          0x0000  0x0000
```

```
0013: ::1          ::B        0x0000  0x0000
0014: ::1          ::D        0x0000  0x0000
0015: ::1          ::F        0x0000  0x0000
0016: ::2          ::1        0x0000  0x0000
0017: ::2          ::3        0x0000  0x0000
0018: ::2          ::5        0x0000  0x0000
0019: ::2          ::7        0x0000  0x0000
0020: ::2          ::9        0x0000  0x0000
0021: ::2          ::B        0x0000  0x0000
0022: ::2          ::D        0x0000  0x0000
0023: ::2          ::F        0x0000  0x0000
0024: ::3          ::1        0x0000  0x0000
0025: ::3          ::3        0x0000  0x0000
0026: ::3          ::5        0x0000  0x0000
0027: ::3          ::7        0x0000  0x0000
0028: ::3          ::9        0x0000  0x0000
0029: ::3          ::B        0x0000  0x0000
0030: ::3          ::D        0x0000  0x0000
0031: ::3          ::F        0x0000  0x0000
```

Table 22: show ipv6 wccp service-number detail Field Descriptions

Field	Description
Protocol Version	The version of WCCP being used by the router in the service group.
State	Indicates whether the WCCP client is operating properly and can be contacted by a router and other clients in the service group.
	When a WCCP client has an incompatible message interval setting, the state of the client is shown as "NOT Usable," followed by a status message describing the reason why the client is not usable.
Redirection	Indicates the redirection method used. WCCP uses GRE or L2 to redirect IP traffic.
Assignment	Indicates the load-balancing method used. WCCP uses HASH or MASK assignment.
Message Interval	The fixed time interval (in seconds)between successive keepalive messages sent from a WCCCP client to a WCCP router. The default time interval is 10 seconds. If the default time interval is configured, the "Message Interval" field is not displayed.
Client timeout	The time (in seconds) that must pass without a WCCP router receiving a keepalive message from a client before the WCCP router considers that client unreachable and removes it from the service group.
Assignment timeout	The time (in seconds) that must pass after the WCCP router detects a failed client and begins to redirect traffic.

Field	Description
Packets Redirected	The number of packets that have been redirected to the content engine.
Connect Time	The amount of time (in hours, minutes, and seconds) the client has been connected to the router.

Examples   The following is sample output from the **show ipv6 wccp interfaces** command:

```
Router# show ipv6 wccp interfaces

WCCP interface configuration:
    FastEthernet0/1/0
        Output services: 2
        Input services: 3
        Mcast services: 1
        Exclude In:      FALSE
```
The table below describes the significant fields shown in the display.

Table 23: show ipv6 wccp interfaces Field Descriptions

Field	Description
Output services	Indicates the number of output services configured on the interface.
Input services	Indicates the number of input services configured on the interface.
Mcast services	Indicates the number of multicast services configured on the interface.
Exclude In	Displays whether traffic on the interface is excluded from redirection.

Examples   The following is sample output from the **show ipv6 wccp web-cache** command:

```
Router# show ipv6 wccp web-cache

Global WCCP information:
    Router information:
        Router Identifier:                2001:DB8:100::1

    Service Identifier: web-cache
        Protocol Version:                 2.01
        Number of Service Group Clients:  2
        Number of Service Group Routers:  1
        Total Packets Redirected:         0
          Process:                        0
          CEF:                            0
        Service mode:                     Open
        Service Access-list:              -none-
```

```
Total Packets Dropped Closed:          0
Redirect access-list:                  -none-
Total Packets Denied Redirect:         0
Total Packets Unassigned:              0
Group access-list:                     -none-
Total Messages Denied to Group:        0
Total Authentication failures:         0
Total GRE Bypassed Packets Received: 0
  Process:                             0
  CEF:                                 0
GRE tunnel interface:                  Tunnel1
```

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

Table 24: show ipv6 wccp web-cache Field Descriptions

Field	Description
Protocol Version	The version of WCCP that is being used by the cache engine in the service group.
Service Identifier	Indicates which service is detailed.
Number of Service Group Clients	Number of clients using the router as their home router.
Number of Service Group Routers	The number of routers in the service group.
Total Packets Redirected	Total number of packets redirected by the router.
Service mode	Indicates whether WCCP open or closed mode is configured.
Service Access-list	The name or number of the service access list that determines which packets will be redirected.
Redirect access-list	The name or number of the access list that determines which packets will be redirected.
Total Packets Denied Redirect	Total number of packets that were not redirected because they did not match the access list.
Total Packets Unassigned	Number of packets that were not redirected because they were not assigned to any cache engine. Packets may not be assigned during initial discovery of cache engines or when a cache is dropped from a cluster.
Group access-list	Indicates which cache engine is allowed to connect to the router.
Total Messages Denied to Group	Indicates the number of packets denied by the *group-list* access list.
Total Authentication failures	The number of instances where a password did not match.

Examples   The following example displays web cache engine information and WCCP traffic counters:

```
Router# show ipv6 wccp web-cache counters

WCCP Service Group Counters:
  Redirected Packets:
    Process:                  0
    CEF:                      0
  Non-Redirected Packets:
    Action - Forward:
      Reason - no assignment:
        Process:              0
        CEF:                  0
    Action - Ignore (forward):
      Reason - redir ACL check:
        Process:              0
        CEF:                  0
    Action - Discard:
      Reason - closed services:
        Process:              0
        CEF:                  0
  GRE Bypassed Packets:
    Process:                  0
    CEF:                      0
  GRE Bypassed Packet Errors:
    Total Errors:
      Process:                0
      CEF:                    0

  WCCP Client Counters:
    WCCP Client ID:           2001:DB8:1::11
      Redirect Assignments:
        Received:             1
        Invalid:              0
        Duplicate:            0
      Redirected Packets:
        Process:              0
        CEF:                  0
      GRE Bypassed Packets:
        Process:              0
        CEF:                  0

    WCCP Client ID:           2001:DB8:1::12
      Redirected Packets:
        Process:              0
        CEF:                  0
      GRE Bypassed Packets:
        Process:              0
        CEF:                  0
```

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

Table 25: show ipv6 wccp web-cache counters Field Descriptions

Field	Description
Redirected Packets	Total number of packets redirected by the router.
Non-Redirected Packets	Total number of packets not redirected by the router.

Examples   The following example displays web cache engine information and WCCP router statistics for the web cache service:

```
Router# show ipv6 wccp web-cache detail

WCCP Client information:
        WCCP Client ID:         2001:DB8:1::11
        Protocol Version:       2.01
        State:                  Usable
        Redirection:            GRE
        Packet Return:          GRE
        Assignment:             HASH
        Connect Time:           1w0d
        Redirected Packets:
          Process:              0
          CEF:                  0
        GRE Bypassed Packets:
          Process:              0
          CEF:                  0
        Hash Allotment:         128 of 256 (50.00%)
        Initial Hash Info:      0000000000000000000000000000000000
                                0000000000000000000000000000000000
        Assigned Hash Info:     5555555555555555555555555555555555
                                5555555555555555555555555555555555

        WCCP Client ID:         2001:DB8:1::12
        Protocol Version:       2.01
        State:                  Usable
        Redirection:            GRE
        Packet Return:          GRE
        Assignment:             HASH
        Connect Time:           1w0d
        Redirected Packets:
          Process:              0
          CEF:                  0
        GRE Bypassed Packets:
          Process:              0
          CEF:                  0
        Hash Allotment:         128 of 256 (50.00%)
        Initial Hash Info:      0000000000000000000000000000000000
                                0000000000000000000000000000000000
        Assigned Hash Info:     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                                AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

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

Table 26: show ipv6 wccp web-cache detail Field Descriptions

Field	Description
WCCP Client Information	The header for the area that contains fields for information on clients.
IP Address	The IP address of the cache engine in the service group.
Protocol Version	The version of WCCP being used by the cache engine in the service group.

Field	Description
State	Indicates whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Redirected Packets	The number of packets that have been redirected to the cache engine.
Connect Time	The amount of time (in hours, minutes, and seconds) the cache engine has been connected to the router.

Examples

The following example displays web cache engine information and WCCP router statistics that include the bypass counters:

```
Router# show ipv6 wccp web-cache detail

WCCP Client information:
        WCCP Client ID:         2001:DB8:1::11
        Protocol Version:       2.01
        State:                  Usable
        Redirection:            GRE
        Packet Return:          GRE
        Assignment:             HASH
        Connect Time:           1w0d
        Redirected Packets:
          Process:              0
          CEF:                  0
        GRE Bypassed Packets:
          Process:              0
          CEF:                  0
        Hash Allotment:         128 of 256 (50.00%)
        Initial Hash Info:      00000000000000000000000000000000
                                00000000000000000000000000000000
        Assigned Hash Info:     55555555555555555555555555555555
                                55555555555555555555555555555555

        WCCP Client ID:         2001:DB8:1::12
        Protocol Version:       2.01
        State:                  Usable
        Redirection:            GRE
        Packet Return:          GRE
        Assignment:             HASH
        Connect Time:           1w0d
        Redirected Packets:
          Process:              0
          CEF:                  0
        GRE Bypassed Packets:
          Process:              0
          CEF:                  0
        Hash Allotment:         128 of 256 (50.00%)
        Initial Hash Info:      00000000000000000000000000000000
                                00000000000000000000000000000000
        Assigned Hash Info:     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                                AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

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

Table 27: show ipv6 wccp web-cache detail Field Descriptions

Field	Description
WCCP Router information	The header for the area that contains fields for the IP address and the version of WCCP associated with the router connected to the cache engine in the service group.
IP Address	The IP address of the router connected to the cache engine in the service group.
Protocol Version	The version of WCCP that is being used by the cache engine in the service group.
WCCP Client Information	The header for the area that contains fields for information on clients.
IP Address	The IP address of the cache engine in the service group.
Protocol Version	The version of WCCP that is being used by the cache engine in the service group.
State	Indicates whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Initial Hash Info	The initial state of the hash bucket assignment.
Assigned Hash Info	The current state of the hash bucket assignment.
Hash Allotment	The percent of buckets assigned to the current cache engine. Both a value and a percent figure are displayed.
Packets Redirected	The number of packets that have been redirected to the cache engine.
Connect Time	The amount of time (in hours, minutes, and seconds) the cache engine has been connected to the router.
Bypassed Packets	The number of packets that have been bypassed. Process and Cisco Express Forwarding are switching paths within Cisco IOS software.

Examples

The following example displays information about a service, including the service definition and all other per-service information:

```
Router# show ipv6 wccp web-cache service

WCCP service information definition:
        Type:          Standard
        Id:            0
        Priority:      240
        Protocol:      6
        Options:       0x00000512
        --------
            Mask/Value sets: 1
            Value elements: 4
            Dst Ports: 80 0 0 0 0 0 0 0
```

Examples

The following example displays information on the configured WCCP services and a summary of their current state:

```
Router# show ipv6 wccp summary

WCCP version 2 enabled, 2 services
Service     Clients   Routers   Assign      Redirect    Bypass
-------     -------   -------   ------      --------    ------
Default routing table (Router Id: 2001:DB8:100::1):
web-cache   2         1         HASH        GRE         GRE
61          2         1         MASK        L2          L2
62          2         1         MASK        L2          L2
```

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

Table 28: show ipv6 wccp summary Field Descriptions

Field	Description
Service	Indicates which service is detailed.
Clients	Indicates the number of cache engines participating in the WCCP service.
Routers	Indicates the number of routers participating in the WCCP service.
Assign	Indicates the load-balancing method used. WCCP uses HASH or MASK assignment.
Redirect	Indicates the redirection method used. WCCP uses GRE or L2 to redirect IP traffic.
Bypass	Indicates the bypass method used. WCCP uses GRE or L2 to return packets to the router.

Related Commands

Command	Description
clear ipv6 wccp	Clears the counter for packets redirected using WCCP.
ipv6 wccp	Enables support of the WCCP service for participation in a service group.
ipv6 wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.
show ipv6 interface	Lists a summary of the IP information and status of an interface.
show ipv6 wccp global counters	Displays global WCCP information for packets that are processed in software.

show ipv6 wccp global counters

To display IPv6 global Web Cache Communication Protocol (WCCP) information for packets that are processed in software, use the **show ipv6 wccp global counters** command in user EXEC or privileged EXEC mode.

show ipv6 wccp global counters

Syntax Description   This command has no arguments or keywords.

Command Modes   User EXEC (>)

Privileged EXEC (#)

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   The **show ipv6 wccp globalcounters** command displays counters for packets that are processed in software.

Examples   The following example displays global WCCP information for packets that are processed in the software:

```
Router# show ipv6 wccp global counters

WCCP Global Counters:
Packets Seen by WCCP
Process:   8
CEF (In):  14
CEF (Out): 0
```

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

Table 29: show ipv6 wccp global counters Field Descriptions

Field	Description
CEF (In)	Number of incoming Cisco Express Forwarding packets
CEF (Out)	Number of outgoing Cisco Express Forwarding packets.

Related Commands

Command	Description
clear ipv6 wccp	Clears the counters for packets redirected using WCCP.
ipv6 wccp	Enables support of the WCCP service for participation in a service group.
ipv6 wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.
show ipv6 interface	Lists a summary of the IP information and the status of an interface.
show ipv6 wccp	Displays the WCCP global configuration and statistics.

show isis ipv6 rib

To display the Intermediate System-to-Intermediate System (IS-IS) IPv6 local routing information base (RIB), use the **show isis ipv6 rib** command in user EXEC or privileged EXEC mode.

show isis ipv6 rib [*ipv6-prefix*]

no show isis ipv6 rib [*ipv6-prefix*]

Syntax Description

ipv6-prefix	(Optional) IPv6 address prefix. This argument must be in the form documented in RFC 2373 with the address specified in hexadecimal, 16-bit values between colons.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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 devices.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(3)M	This command was modified. Filtered routes are now represented by a hyphen (-).

Usage Guidelines

When the optional *ipv6-prefix* argument is not used, the complete Intermediate System-to-Intermediate System (IS-IS) IPv6 RIB is displayed. When an optional IPv6 prefix is supplied, only the entry matching that prefix is displayed.

Only the optimal paths will be installed in the master IPv6 RIB as IS-IS routes.

Examples   The following is sample output from the **show isis ipv6 rib** command. An asterisk (*) indicates prefixes that have been installed and a hyphen (-) indicates prefixes that have been filtered out in the master IPv6 RIB as IS-IS routes. Following each prefix is a list of all paths in order of preference, with optimal paths listed first and suboptimal paths listed after optimal paths.

```
Device# show isis ipv6 rib

IS-IS IPv6 process , local RIB
  11::1/128
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3]
  20::/64
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L1  metric 20 tag 0 LSP [4/2]
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3]
* 22::2/128
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L1  metric 20 tag 0 LSP [4/2] -
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3] -
  2001:DB8::/64
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L1  metric 20 tag 0 LSP [4/2]
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3]
```

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

Table 30: show isis ipv6 rib Field Descriptions

Field	Description
11::1/128	IPv6 prefix that is stored within the IS-IS local RIB.
via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0	IPv6 address of the next hop—in this instance, Ethernet0/0.
type	Type of path: • L1—Level 1 • L2—Level 2
tag	Priority of the IPv6 prefix. All prefixes have a tag 0 priority unless otherwise configured.
LSP [3/3]	Link-state packet (LSP). The numbers following LSP indicate the LSP index and LSP version, respectively.
*	Prefixes that have been installed in the master IPv6 RIB as IS-IS routes.
-	Route paths that are filtered out.

Related Commands

Command	Description
distribute-list in (IP)	Filters routes received in incoming updates.
show isis ip rib	Displays the IS-IS IPv4 local RIB.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

show monitor event-trace vpn-mapper

To display event trace messages for IPv6 virtual private networks (VPNs), use the **show monitor event-trace vpn-mapper**command in privileged EXEC mode.

show monitor event-trace vpn-mapper {**latest**| **all**}

Syntax Description

latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
all	Displays all event trace messages currently in memory for the specified component.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB1	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **show monitor event-trace** command to display trace message information about IPv6 VPNs.

Examples

The following example allows event trace messages for IPv6 VPNs to be displayed:

```
Router# show monitor event-trace vpn-mapper
```

show ospfv3 border-routers

To display the internal Open Shortest Path First version 3 (OSPFv3) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ospfv3 border-routers** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name*| *****}] **border-routers**

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.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A VRF name of "*" displays information for all VRFs, including the global table.

Command Modes   Privileged EXEC

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.
Cisco IOS Release 15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS Release 15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following examples enables the display of the internal OSPFv3 routing table entries to an ABR and ASBR:

```
Router# show ospfv3 border-routers
```

show ospfv3 database

To display lists of information related to the Open Shortest Path First version 3 (OSPFv3) database for a specific router, use the **show ospfv3 database** command in user EXEC or privileged EXEC mode. The various forms of this command deliver information about different OSPFv3 link-state advertisements (LSAs).

{**show ospfv3** [*process-id* [*area-id*]] [*address-family*] [**vrf** {*vrf-name*| *****}]**database** [**database-summary**| **internal**| **external** [ipv6-prefix] [*link-state-id*]]| **grace**| **inter-area prefix** [ipv6-prefix| *link-state-id*]| **inter-area router** [**destination-router-id**| *link-state-id*]| **link** [**interface** *interface-name*| *link-state-id*]| **network** [*link-state-id*]| **nssa-external** [*ipv6-prefix*] [*link-state-id*]| **prefix** [**ref-lsa** {**router**| **network**}| *link-state-id*]| **promiscuous**| **router** [*link-state-id*]| **unknown** [{**area**| **as**| **link**} [*link-state-id*]] [**adv-router** *router-id*] [**self-originate**]}

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.
area-id	(Optional) Displays information only about a specified area. The *area-id* argument can only be used if the *process-id* argument is specified.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *}*	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
database-summary	(Optional) Displays how many of each type of LSAs exist for each area in the database, and the total.
internal	(Optional) Internal LSA information.
external	(Optional) Displays information only about the external LSAs.
ipv6-prefix	(Optional) Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
grace	(Optional) Displays information about OSPFv3 graceful restart.

link-state-id	(Optional) An integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
inter-area prefix	(Optional) Displays information only about LSAs based on inter-area prefix LSAs.
inter-area router	(Optional) Displays information only about LSAs based on inter-area router LSAs.
destination-router-id	(Optional) The specified destination router ID.
link	(Optional) Displays information about the link LSAs.
interface	(Optional) Displays information about the LSAs filtered by interface context.
interface-name	(Optional) Specifies the LSA interface.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.
prefix	(Optional) Displays information on the intra-area-prefix LSAs.
promiscuous	(Optional) Displays temporary LSAs in a Mobile Ad Hoc Network (MANET).
ref-lsa {**router**	**network**}	(Optional) Further filters the prefix LSA type.
router	(Optional) Displays information only about the router LSAs.
unknown	(Optional) Displays all LSAs with unknown types.
area	(Optional) Filters unknown area LSAs.
as	(Optional) Filters unknown autonomous system (AS) LSAs.
link	(Optional) When following the **unknown** keyword, the **link** keyword filters link-scope LSAs.
adv-router *router-id*	(Optional) Displays all the LSAs of the advertising router. This argument must be in the form documented in RFC 2740 where the address is specified in hexadecimal using 16-bit values between colons.

self-originate	(Optional) Displays only self-originated LSAs (from the local router).

Command Modes   User EXEC Privileged EXEC

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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines   The **adv-router** keyword requires a router ID. The **self-originate** keyword displays only those LSAs that originated from the local router. Both of these keywords can be appended to all other keywords used with the **show ospfv3 database**database command to provide more detailed information.

Examples   The following is sample output from the **show ospfv3 database** command when no arguments or keywords are used:

```
Router# show ospfv3 database
            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)
                Router Link States (Area 0)
ADV Router         Age          Seq#          Fragment ID    Link count  Bits
172.16.4.4         239          0x80000003    0              1           B
172.16.6.6         239          0x80000003    0              1           B
            Inter Area Prefix Link States (Area 0)
ADV Router         Age          Seq#          Prefix
172.16.4.4         249          0x80000001    FEC0:3344::/32
172.16.4.4         219          0x80000001    FEC0:3366::/32
172.16.6.6         247          0x80000001    FEC0:3366::/32
172.16.6.6         193          0x80000001    FEC0:3344::/32
172.16.6.6         82           0x80000001    FEC0::/32
            Inter Area Router Link States (Area 0)
ADV Router         Age          Seq#          Link ID      Dest RtrID
172.16.4.4         219          0x80000001    50529027     172.16.3.3
172.16.6.6         193          0x80000001    50529027     172.16.3.3


            Link (Type-8) Link States (Area 0)
ADV Router         Age          Seq#          Link ID      Interface
172.16.4.4         242          0x80000002    14           PO4/0
172.16.6.6         252          0x80000002    14           PO4/0
            Intra Area Prefix Link States (Area 0)
ADV Router         Age          Seq#          Link ID      Ref-lstype   Ref-LSID
172.16.4.4         242          0x80000002    0            0x2001       0
172.16.6.6         252          0x80000002    0            0x2001       0
```

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

Table 31: show ospfv3 database Field Descriptions

Field	Description
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Link ID	Interface ID number.
Ref-lstype	Referenced link-state type.
Ref-LSID	Referenced link-state ID.

show ospfv3 events

To display detailed information about Open Shortest Path First version 3 (OSPFv3) events, use the **show ospfv3 events**command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name*| *****}]**events** [**generic**| **interface**| **lsa**| **neighbor**| **reverse**| **rib**| **spf**]

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.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
generic	(Optional) Generic information regarding OSPFv3 events.
interface	(Optional) Interface state change events, including old and new states.
lsa	(Optional) LSA arrival and LSA generation events.
neighbor	(Optional) Neighbor state change events, including old and new states.
reverse	(Optional) Keyword to allow the display of events in reverse-from the latest to the oldest or from oldest to the latest.
rib	(Optional) Routing Information Base (RIB) update, delete, and redistribution events.
spf	(Optional) Scheduling and SPF run events.

Command Modes

Privileged EXEC

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.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
	15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines   An OSPFv3 event log is kept for every OSPFv3 instance. If you enter the **show ospfv3 events** command without any keywords, all information in the OSPFv3 event log is displayed. Use the keywords to filter specific information.

Examples   The following example enables the display of information about OSPFv3 events:

```
Router# show ospfv3 events
```

show ospfv3 flood-list

To display a list of Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) waiting to be flooded over an interface, use the **s how ospfv3 flood-list**command in privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] [**vrf** {*vrf-name*| *****}]**flood-list** *interface-type interface-number*

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.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
interface-type	Interface type over which the LSAs will be flooded.
interface-number	Interface number over which the LSAs will be flooded.

Command Modes

Privileged EXEC

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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Release	Modification
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines   Use this command to display OSPFv3 packet pacing.

Examples   The following displays a list of OSPFv3 LSAs waiting to be flooded over an interface:

```
Router# show ospfv3 flood-list
```

show ospfv3 graceful-restart

To display Open Shortest Path First version 3 (OSPFv3) graceful restart information, use the **show ospfv3 graceful-restart** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name*| ***}]**graceful-restart**

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.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name*	***}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.

Command Modes   Privileged EXEC

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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines   Use the **show ospfv3 graceful-restart** command to discover information about the OSPFv3 graceful restart feature.

Examples   The following example displays OSPFv3 graceful restart information:

```
Router# show ospfv3 graceful-restart
```

show ospfv3 interface

To display Open Shortest Path First version 3 (OSPFv3)-related interface information, use the **show ospfv3 interface** command in privileged mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] [**vrf** {*vrf-name*| *****}]**interface** [*type number*] **[brief]**

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.
area-id	(Optional) Displays information about a specified area only.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name*	*****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
type number	(Optional) Interface type and number.
brief	(Optional) Displays brief overview information for OSPFv3 interfaces, states, addresses and masks, and areas on the router.

Command Modes   Privileged EXEC

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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Release	Modification
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following is sample output from the **show ospfv3 interface** command for a Mobile Ad Hoc Network (MANET) environment:

```
Router# show ospfv3 interface
Ethernet0/0 is up, line protocol is up
Link Local Address FE80::A8BB:CCFF:FE01:5500, Interface ID 3
Area 0, Process ID 100, Instance ID 0, Router ID 172.16.3.3
Network Type MANET, Cost: 10 (dynamic), Cost Hysteresis: Disabled
Cost Weights: Throughput 100, Resources 100, Latency 100, L2-factor 100
Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
Incremental Hello is enabled
Local SCS number 1
Relaying enabled
Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
Router#
```

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

Table 32: show ospfv3 interface Field Descriptions

Field	Description
Ethernet0/0	Status of the physical link and the operational status of the protocol.
Link Local Address	Interface IPv6 address.
Area 0, Process ID 100, Instance ID 0, Router ID 172.16.3.3	Area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type MANET, Cost: 10 (dynamic), Cost hysteresis: Disabled	Network type and link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Timer intervals configured	Configuration of timer intervals, including hello-increment and dead-interval.

Field	Description
Hello due in 00:00:01	Number of seconds until the next hello packet is sent from this interface.
Supports Link-local Signaling (LLS)	Indicates that LLS is supported.
Last flood scan length is 2, maximum is 2	Indicates length of last flood scan and the maximum length.
Last flood scan time is 0 msec, maximum is 0 msec	Indicates how many milliseconds the last flood scan occurred and the maximum time length.
Neighbor Count	Count of network neighbors and a list of adjacent neighbors.
Adjacent with neighbor 2.2.2.2	Lists the adjacent neighbor.
Suppress hello for 0 neighbor(s)	Indicates the number of neighbors to suppress hello messages

show ospfv3 max-metric

To display Open Shortest Path First version 3 (OSPFv3) maximum metric origination information, use the **show ospfv3 max-metric** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name*| *****}]**max-metric**

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.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.

Command Modes

User EXEC Privileged EXEC

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(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The information displayed by the **show ospfv3 max-metric** command is useful in debugging OSPFv3 routing operations. You can also use the **show ipv6 ospf max-metric** command display the same information as the **show ospfv3 max-metric** command.

Examples   The following is sample output from the **show ospfv3 max-metric** command:

```
Router# show ospfv3 1 max-metric
Routing Process "ospfv3 1" with ID 192.168.2.1
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Originating router-LSAs with maximum metric, Time remaining: 00:01:18
    Condition: on startup while BGP is converging, State: active
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        SPF algorithm executed 2 times
        Number of LSA 6. Checksum Sum 0x0327C7
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

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

Table 33: show ospfv3 max-metric command

Field	Description
Routing Process "ospfv3 1" with ID 192.168.2.1	The routing process specified by process ID.
Event-log enabled, Maximum number of events: 1000, Mode: cyclic	Configuration for this OSPFv3 process.
Originating router-LSAs with maximum metric, Time remaining: 00:01:18	
Condition: on startup while BGP is converging, State: active	The router advertises a max metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired.

show ospfv3 neighbor

To display Open Shortest Path First for IPv6 (OSPFv3) neighbor information on a per-interface basis, use the **show ospfv3 neighbor** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] [**vrf** {*vrf-name*| *****}] **neighbor** [*interface-type interface-number*] [*neighbor-id*] **[detail]**[**summary** [**per-instance**]]

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.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
interface-type interface-number	(Optional) Interface type and number.
neighbor-id	(Optional) Neighbor ID.
detail	(Optional) Displays all neighbors in detail (lists all neighbors).
summary	(Optional) Displays total number summary of all neighbors.
per-instance	(Optional) Displays total number of neighbors in each neighbor state. The output is printed for each configured OSPF instance separately.

Command Modes　　　User EXEC Privileged EXEC

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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M. This command was modified. The **summary** and **per-instance** keywords were added.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S. This command was modified. The **summary** and **per-instance** keywords were added.

Examples

The following is sample output from the **show ospfv3 neighbor** command:

```
Device# show ospfv3 neighbor

OSPFv3 Router with ID (42.1.1.1) (Process ID 42)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
44.4.4.4         1    FULL/  -        00:00:39    12              vm1
OSPFv3 Router with ID (1.1.1.1) (Process ID 100)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
4.4.4.4          1    FULL/  -        00:00:35    12              vm1
```

The following is sample output from the **show ospfv3 neighbor** command with the **detail** keyword for a Mobile Ad Hoc Network (MANET) environment:

```
Device# show ospfv3 neighbor detail
Neighbor 42.4.4.4, interface address 4.4.4.4
In the process ID 42 area 0 via interface vmi1
Neighbor: interface-id 12, link-local address FE80::A8BB:CCFF:FE01:5800
Neighbor priority is 1, State is FULL, 6 state changes
Options is 0x000F12 in Hello (E-Bit, R-bit, AF-Bit, L-Bit, I-Bit, F-Bit)
Options is 0x000112 in DBD (E-Bit, R-bit, AF-Bit)
Dead timer due in 00:00:33
Neighbor is up for 00:09:43
Index 1/1/1, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor is incremental Hello capable
Last known SCS number 1
Neighbor's willingness 128
We are standby relay for the neighbor
This neighbor is standby relay for us
Neighbor is running Manet Version 10
Neighbor 4.4.4.4
In the process ID 100 area 0 via interface vmi1
Neighbor: interface-id 12, link-local address FE80::A8BB:CCFF:FE01:5800
Neighbor priority is 1, State is FULL, 6 state changes
Options is 0x000E13 in Hello (V6-Bit, E-Bit, R-bit, L-Bit, I-Bit, F-Bit)
Options is 0x000013 in DBD (V6-Bit, E-Bit, R-bit)
```

```
Dead timer due in 00:00:37
Neighbor is up for 00:09:43
Index 1/1/1, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor is incremental Hello capable
Last known SCS number 1
Neighbor's willingness 128
Two-hop neighbors:
5.5.5.5
We are standby relay for the neighbor
This neighbor is active relay for us
Neighbor is running Manet Version 10
Selective Peering is enabled
1 paths to this neighbor
Neighbor peering state: Slave, local peering state: Master,
Default cost metric is 0
Minimum incremental cost is 10
```

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

Table 34: show ospfv3 neighbor Field Descriptions

Field	Description
Neighbor ID; Neighbor	Neighbor device ID.
In the area	Area and interface through which the OSPFv3 neighbor is known.
Pri; Neighbor priority	Device priority of the neighbor, neighbor state.
State	OSPFv3 state.
State changes	Number of state changes since the neighbor was created.
Options	Hello packet options field contents (E-bit only). Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)
Dead timer due in	Expected time before Cisco IOS software declares the neighbor dead.
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into two-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in the retransmission queue.
number of retransmission	Number of times update packets have been resent during flooding.
First	Memory location of the flooding details.

Field	Description
Next	Memory location of the flooding details.
Last retransmission scan length	Number of link state advertisements (LSAs) in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build last retransmission packet.
maximum	Maximum time taken to build any retransmission packet.
Neighbor is incremental Hello capable	The MANET neighbor interface is capable of receiving increment hello messages. A neighbor must be capable of sending and receiving incremental hello packets to be a full neighbor on a MANET interface.
Last known SCS number 1	Indicates the last received MANET state. The State Change Sequence number is included in the incremental hello packet.
Neighbor's willingness 128	Indicates the neighbors willingness to act as an active relay for this device, on a scale of 0 (not willing) to 255 (always willing). Willingness is used as a tiebreaker when electing an active relay.
We are standby relay for neighbor	Indicates that this device will not flood LSAs received from this neighbor until one or more of its neighbors fails to acknowledge receiving the LSA flood from another neighbor.
Neighbor is running Manet Version 10	Indicates the MANET version number. Devices cannot establish full adjacency unless they are running the same MANET version.
Two-hop neighbors	Lists the device IDs of all full neighbors of the specified device that are not also neighbors of this device.
Selective Peering is enabled	The MANET interface has selective peering enabled.

Field	Description
1 paths to this neighbor	Indicates the number of unique paths to this device that exist in the routing table.
	This number might exceed the redundancy level configured for this OSPFv3 process.
Neighbor peering state...	Indicates which device is entitled to make the selective peering decision.
	Generally speaking, the entitled device has the smaller number of full neighbors at the time the devices discover each other.
Default cost metric is 0	Indicates the maximum OSPFv3 cost to a new neighbor to be considered for selective peering.
	If 0, a threshold OSPFv3 cost is not required for consideration.
Minimum incremental cost is 10	Indicates the minimum cost increment for the specified interface.

The following is sample output from the **show ospfv3 neighbor summary** command:

```
Device# show ospfv3 neighbor summary

OSPFv3 1 address-family ipv6 (router-id 10.4.9.158)

DOWN          0
ATTEMPT       0
INIT          0
2WAY          0
EXSTART       0
EXCHANGE      0
LOADING       0
FULL          1
Total count  1    (Undergoing GR 0)
```

The following is sample output from the **show ospfv3 neighbor summary per-instance** command:

```
Device# show ospfv3 neighbor summary per-instance

OSPFv3 1 address-family ipv6 (router-id 10.4.9.158)

DOWN          0
ATTEMPT       0
INIT          0
2WAY          0
EXSTART       0
EXCHANGE      0
LOADING       0
FULL          1
Total count  0    (Undergoing GR 0)


Neighbor summary for selected OSPFv3 processes

DOWN          0
ATTEMPT       0
```

```
INIT          0
2WAY          0
EXSTART       0
EXCHANGE      0
LOADING       0
FULL          1
Total count  0     (Undergoing GR 0)
```

Table 35: show ospfv3 neighbor summary and show ospfv3 neighbor summary per-instance Field Descriptions

Field	Description
DOWN	No information (hellos) has been received from this neighbor, but hello packets can still be sent to the neighbor in this state.
ATTEMPT	This state is only valid for manually configured neighbors in a Non-Broadcast Multi-Access (NBMA) environment. In Attempt state, the device sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval.
INIT	This state specifies that the device has received a hello packet from its neighbor, but the receiving device's ID was not included in the hello packet. When a device receives a hello packet from a neighbor, it should list the sender's device ID in its hello packet as an acknowledgment that it received a valid hello packet.
2WAY	This state designates that bi-directional communication has been established between two devices.
EXSTART	This state is the first step in creating an adjacency between the two neighboring devices. The goal of this step is to decide which device is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies.

Field	Description
EXCHANGE	In this state, OSPF devices exchange database descriptor (DBD) packets. Database descriptors contain link-state advertisement (LSA) headers only and describe the contents of the entire link-state database. Each DBD packet has a sequence number which can be incremented only by master which is explicitly acknowledged by slave. Devices also send link-state request packets and link-state update packets (which contain the entire LSA) in this state. The contents of the DBD received are compared to the information contained in the devices link-state database to check if new or more current link-state information is available with the neighbor.
LOADING	In this state, the actual exchange of link state information occurs. Based on the information provided by the DBDs, devices send link-state request packets. The neighbor then provides the requested link-state information in link-state update packets. During the adjacency, if a device receives an outdated or missing LSA, it requests that LSA by sending a link-state request packet. All link-state update packets are acknowledged.
FULL	In this state, devices are fully adjacent with each other. All the device and network LSAs are exchanged and the devices' databases are fully synchronized. Full is the normal state for an OSPF device. If a device is stuck in another state, it's an indication that there are problems in forming adjacencies. The only exception to this is the 2-way state, which is normal in a broadcast network. Devices achieve the full state with their DR and BDR only. Neighbors always see each other as 2-way.

show ospfv3 request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ospfv3 request-list**command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] [**vrf** {*vrf-name*| *****}]**request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
neighbor	(Optional) Displays the list of all LSAs requested by the router from this neighbor.
interface	(Optional) Displays the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Displays the list of all LSAs requested by the router on this interface, from this neighbor.

Command Modes

User EXEC Privileged EXEC

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.

Release	Modification
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines   The information displayed by the **show ospfv3 request-list** command is useful in debugging OSPFv3 routing operations.

Examples   The following example shows information about the LSAs requested by the router:

```
Router# show ospfv3 request-list

          OSPFv3 Router with ID (192.168.255.5) (Process ID 1)
 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600
 Type   LS ID          ADV RTR         Seq NO      Age     Checksum
 1      0.0.0.0        192.168.255.3   0x800000C2  1       0x0014C5
 1      0.0.0.0        192.168.255.2   0x800000C8  0       0x000BCA
 1      0.0.0.0        192.168.255.1   0x800000C5  1       0x008CD1
 2      0.0.0.3        192.168.255.3   0x800000A9  774     0x0058C0
 2      0.0.0.2        192.168.255.3   0x800000B7  1       0x003A63
```
The table below describes the significant fields shown in the display.

Table 36: show ospfv3 request-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.5) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ospfv3 retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the **show ospfv3 retransmission-list**command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] [**vrf** {*vrf-name*| *****}]**retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name*	*****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.
interface	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.
interface neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.

Command Modes   User EXEC Privileged EXEC

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.

Release	Modification
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The information displayed by the **show ospfv3 retransmission-list** command is useful in debugging Open Shortest Path First version 3 (OSPFv3) routing operations.

Examples

The following is sample output from the **show ospfv3 retransmission-list** command:

```
Router# show ospfv3 retransmission-list

        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)
Neighbor 192.168.255.1, interface Ethernet0/0
Link state retransmission due in 3759 msec, Queue length 1
Type    LS ID            ADV RTR         Seq NO      Age     Checksum
0x2001  0                192.168.255.2   0x80000222  1       0x00AE52
```
The table below describes the significant fields shown in the display.

Table 37: show ospfv3 retransmission-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.2) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Link state retransmission due in	Length of time before next link-state transmission.
Queue length	Number of elements in the retransmission queue.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of the LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ospfv3 statistic

To display Open Shortest Path First version 3 (OSPFv3) shortest path first (SPF) calculation statistics, use the **show ospfv3 statistic** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name*| *****}]**statistic [detail]**

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.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
detail	(Optional) Displays statistics separately for each OSPFv3 area and includes additional, more detailed statistics.

Command Modes

User EXEC (>) Privileged EXEC (#)

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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines   The **show ospfv3 statistics** command provides important information about SPF calculations and the events that trigger them. This information can be meaningful for both OSPF network maintenance and troubleshooting. For example, entering the **show ospfv3 statistics** command is recommended as the first troubleshooting step for link-state advertisement (LSA) flapping.

Examples   The following example provides detailed statistics for each OSPFv3 area:

```
Router# show ospfv3 statistics detail
  Area 0: SPF algorithm executed 3 times
SPF 1 executed 00:06:57 ago, SPF type Full
  SPF calculation time (in msec):
  SPT     Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0       0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R N SN SA L
  LSAs changed 1
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  10.2.2.2/0(R)
SPF 2 executed 00:06:47 ago, SPF type Full
  SPF calculation time (in msec):
  SPT     Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0       0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:1 SN:0 SA:0 X7:0
  Change record R L P
  LSAs changed 4
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  10.2.2.2/2(L) 10.2.2.2/0(R) 10.2.2.2/2(L) 10.2.2.2/0(P)
```

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

Table 38: show ospfv3 statistics Field Descriptions

Field	Description
Area	OSPF area ID.
SPF	Number of SPF algorithms executed in the OSPF area. The number increases by one for each SPF algorithm that is executed in the area.
Executed ago	Time in milliseconds that has passed between the start of the SPF algorithm execution and the current time.
SPF type	SPF type can be Full or Incremental.
SPT	Time in milliseconds required to compute the first stage of the SPF algorithm (to build a short path tree). The SPT time plus the time required to process links to stub networks equals the Intra time.

Field	Description
Ext	Time in milliseconds for the SPF algorithm to process external and not so stubby area (NSSA) LSAs and to install external and NSSA routes in the routing table.
Total	Total duration time in milliseconds for the SPF algorithm process.
LSIDs processed	Number of LSAs processed during the SPF calculation: • N--Network LSA. • R--Router LSA. • SA--Summary Autonomous System Boundary Router (ASBR) (SA) LSA. • SN--Summary Network (SN) LSA. • Stub--Stub links. • X7--External Type-7 (X7) LSA.

show ospfv3 summary-prefix

To display a list of all summary address redistribution information configured under an Open Shortest Path First version 3 (OSPFv3) process, use the **show ospfv3 summary-prefix**command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name*| *****}]**summary-prefix**

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.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.

Command Modes

User EXEC Privileged EXEC

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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The *process-id* argument can be entered as a decimal number or as an IPv6 address format.

Examples

The following is sample output from the **show ospfv3 summary-prefix** command:

```
Router# show ospfv3 summary-prefix

OSPFv3 Process 1, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

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

Table 39: show ospfv3 summary-prefix Field Descriptions

Field	Description
OSPFv3 Process	Process ID of the router for which information is displayed.
Metric	Metric used to reach the destination router.
Type	Type of link-state advertisement (LSA).
Tag	LSA tag.

show ospfv3 timers rate-limit

To display all of the link-state advertisements (LSAs) in the rate limit queue, use the **show ospfv3 timers rate-limit**command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name*| *****}]**timers rate-limit**

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.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.

Command Modes

Privileged EXEC

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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **show ospfv3 timers rate-limit** command to discover when LSAs in the queue will be sent.

Examples

The following is sample output from the **show ospfv3 timers rate-limit**command:

```
Router# show ospfv3 timers rate-limit
List of LSAs that are in rate limit Queue
    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
```
The table below describes the significant fields shown in the display.

Table 40: show ospfv3 timers rate-limit Field Descriptions

Field	Description
LSAID	ID of the LSA.
Type	Type of LSA.
Adv Rtr	ID of the advertising router.
Due in:	When the LSA is scheduled to be sent (in hours:minutes:seconds).

show ospfv3 traffic

To display Open Shortest Path First version 3 (OSPFv3) traffic statistics, use the **show ospfv3 traffic**command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name*| ***}**]traffic** [*interface-type interface-number*]

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.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name*	***}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
interface-type interface-number	(Optional) Type and number associated with a specific OSPFv3 interface.

Command Default

When the **show ospfv3 traffic** command is entered without any arguments, global OSPFv3 traffic statistics are displayed, including queue statistics for each OSPFv3 process, statistics for each interface, and per OSPFv3 process statistics.

Command Modes

Privileged EXEC

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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Release	Modification
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines   You can limit the displayed traffic statistics to those for a specific OSPFv3 process by entering a value for the *process-id* argument, or you can limit output to traffic statistics for a specific interface associated with an OSPFv3 process by entering values for the *interface-type* and *interface-number* arguments.

Examples   The following example shows the display output for the **show ospfv3 traffic** command for OSPFv3:

```
Router# show ospfv3 traffic
OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored
  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
        OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      5                    196
  RX DB des     4                    172
  RX LS req     1                    52
  RX LS upd     4                    320
  RX LS ack     2                    112
  RX Total      16                   852
  TX Failed     0                    0
  TX Hello      8                    304
  TX DB des     3                    144
  TX LS req     1                    52
  TX LS upd     3                    252
  TX LS ack     3                    148
  TX Total      18                   900
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
    Interface Ethernet0/0
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      6                    240
  RX DB des     3                    144
  RX LS req     1                    52
  RX LS upd     5                    372
  RX LS ack     2                    152
  RX Total      17                   960
  TX Failed     0                    0
  TX Hello      11                   420
  TX DB des     9                    312
  TX LS req     1                    52
  TX LS upd     5                    376
  TX LS ack     3                    148
```

```
   TX Total      29                1308
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 6:
OSPFv3 packets received/sent
  Type          Packets            Bytes
  RX Invalid    0                  0
  RX Hello      11                 436
  RX DB des     7                  316
  RX LS req     2                  104
  RX LS upd     9                  692
  RX LS ack     4                  264
  RX Total      33                 1812
  TX Failed     0                  0
  TX Hello      19                 724
  TX DB des     12                 456
  TX LS req     2                  104
  TX LS upd     8                  628
  TX LS ack     6                  296
  TX Total      47                 2208
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

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

Table 41: show ospfv3 traffic Field Descriptions

Field	Description
OSPFv3 statistics	Traffic statistics accumulated for all OSPFv3 processes running on the router. To ensure compatibility with the **show ip traffic** command, only checksum errors are displayed. Identifies the route map name.
OSPFv3 queues statistic for process ID	Queue statistics specific to Cisco IOS software.
Hello queue	Statistics for the internal Cisco IOS queue between the packet switching code (process IP Input) and the OSPFv3 hello process for all received OSPFv3 packets.
Router queue	Statistics for the internal Cisco IOS queue between the OSPFv3 hello process and the OSPFv3 router for all received OSPFv3 packets except OSPFv3 hellos.
queue size	Actual size of the queue.
queue limit	Maximum allowed size of the queue.
queue max size	Maximum recorded size of the queue.

Field	Description
Interface statistics	Per-interface traffic statistics for all interfaces that belong to the specific OSPFv3 process ID.
OSPFv3 packets received/sent	Number of OSPFv3 packets received and sent on the interface, sorted by packet types.
OSPFv3 header errors	Packet appears in this section if it was discarded because of an error in the header of an OSPFv3 packet. The discarded packet is counted under the appropriate discard reason.
OSPFv3 LSA errors	Packet appears in this section if it was discarded because of an error in the header of an OSPFv3 link-state advertisement (LSA). The discarded packet is counted under the appropriate discard reason.
Summary traffic statistics for process ID	Summary traffic statistics accumulated for an OSPFv3 process. **Note** The OSPFv3 process ID is a unique value assigned to the OSPFv3 process in the configuration. The value for the received errors is the sum of the OSPFv3 header errors that are detected by the OSPFv3 process, unlike the sum of the checksum errors that are listed in the global OSPFv3 statistics.

show ospfv3 virtual-links

To display parameters and the current state of Open Shortest Path First version 3 (OSPFv3) virtual links, use the **show ospfv3 virtual-links** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name*| *****}]**virtual-links**

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.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.

Command Modes

User EXEC Privileged EXEC

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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The information displayed by the **show ospfv3 virtual-links** command is useful in debugging OSPFv3 routing operations.

Examples   The following is sample output from the **show ospfv3 virtual-links** command:

```
Router# show ospfv3 virtual-links
Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```
The table below describes the significant fields shown in the display.

Table 42: show ospfv3 virtual-links Field Descriptions

Field	Description
Virtual Link OSPF_VL0 to router 172.16.6.6 is up	Specifies the OSPFv3 neighbor, and if the link to that neighbor is up or down.
Interface ID	Interface ID and IPv6 address of the router.
Transit area 2	The transit area through which the virtual link is formed.
via interface ATM3/0	The interface through which the virtual link is formed.
Cost of using 1	The cost of reaching the OSPFv3 neighbor through the virtual link.
Transmit Delay is 1 sec	The transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	The state of the OSPFv3 neighbor.
Timer intervals...	The various timer intervals configured for the link.
Hello due in 0:00:06	When the next hello is expected from the neighbor.

The following sample output from the **show ospfv3 virtual-links** command has two virtual links. One is protected by authentication, and the other is protected by encryption. <<This is show ipv6 ospf virtual-links output--should it be modified/replaced?>>

```
Router# show ospfv3 virtual-links
Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
  Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial12/0, Cost of using 64
  NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
    Adjacency State FULL (Hello suppressed)
    Index 1/2/4, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
```

```
      Last retransmission scan length is 1, maximum is 1
      Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
    Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
    Run as demand circuit
    DoNotAge LSA allowed.
    Transit area 1, via interface Serial11/0, Cost of using 128
    MD5 authentication SPI 940, secure socket UP (errors: 0)
    Transmit Delay is 1 sec, State POINT_TO_POINT,
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Adjacency State FULL (Hello suppressed)
      Index 1/1/3, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
      Last retransmission scan length is 1, maximum is 1
      Last retransmission scan time is 0 msec, maximum is 0 msec
```

show platform 6rd tunnel-endpt

To display IPv6 rapid deployment (6RD) information about a tunnel end point, use the **show platform 6rd tunnel-endpt** command in the Privileged EXEC mode.

show platform 6rd tunnel-endpt

Syntax Description

tunnel-endpt	Displays 6rd tunnel end points.

Command Default   None

Command Modes   Privileged EXEC

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco 7600 series routers.

Examples   This example displays the total number of tunnel end points configured.

```
Device#show platform 6rd tunnel-endpt
6rd End-pt in use: 1
6rd End-pt in use: 2
6rd End-pt in use: 3
6rd End-pt in use: 4
6rd End-pt in use: 5
6rd End-pt in use: 6
6rd End-pt in use: 7
6rd End-pt in use: 8
6rd End-pt in use: 9
--More--
6rd End-pt in use: 108
6rd End-pt in use: 109
6rd End-pt in use: 110
Total 6rd End-pt in use: 110
```

Related Commands

Command	Description
show tunnel 6rd destination	Translates a 6RD prefix to the corresponding IPv4 destination.
tunnel 6rd prefix	Specifies the common IPv6 prefix on IPv6 6RD tunnels.
tunnel mode ipv6ip	Configures a static IPv6 tunnel interface.

Command	Description
tunnel source	Sets the source address for a tunnel interface.

show platform software ipv6-multicast

To display information about the platform software for IPv6 multicast, use the **show platform software ipv6-multicast**command in privileged EXEC mode.

show platform software ipv6-multicast {**acl-exception**| **acl-table**| **capability**| **connected**| **shared-adjacencies**| **statistics**| **summary**}

Syntax Description

acl-exception	Displays the IPv6-multicast entries that were switched in the software due to ACL exceptions.
acl-table	Displays the IPv6-multicast access list (ACL) request table entries.
capability	Displays the hardware capabilities.
connected	Displays the IPv6-multicast subnet/connected hardware entries.
shared-adjacencies	Displays the IPv6-multicast shared adjacencies.
statistics	Displays the internal software-based statistics.
summary	Displays the IPv6-multicast hardware-shortcut count.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.2(18)SXD	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(18)SXE	This command was changed as follows: • Add the **acl-exception**, **acl-table**, and the **statistics**keywords on the Supervisor Engine 720 only. • Update the **show platform software ipv6-multicast capability** command output to include replication information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples   This example shows how to display the IPv6-hardware capabilities:

```
Router# show platform software ipv6-multicast capability
 Hardware switching for ipv6 is Enabled
 (S,G) forwarding for ipv6 supported using Netflow
 (*,G) bridging for ipv6 is supported using Fib
 Directly-connected entries for IPv6 is supported using ACL-TCAM.
Current System HW Replication Mode : Egress
Audo-detection of Replication Mode : ON
Slot Replication-Capability Replication-Mode
   2 Egress                 Egress
   5 Egress                 Egress
```

This example shows how to display the IPv6-multicast subnet/connected-hardware entries:

```
Router# show platform software ipv6-multicast connected
IPv6 Multicast Subnet entries
Flags : H - Installed in ACL-TCAM
        X - Not installed in ACL-TCAM due to
            label-full exception
Interface: Vlan40 [ H ]
        S:40::1 G:FF00::
        S:0:5000::2 G:FF00::
        S:5000::2 G:FF00::
Interface: Vlan30 [ H ]
        S:30::1 G:FF00::
Interface: Vlan20 [ H ]
        S:20::1 G:FF00::
Interface: Vlan10 [ H ]
        S:10::1 G:FF00::
```

This example shows how to display the IPv6-multicast shared adjacencies:

```
Router# show platform software ipv6-multicast shared-adjacencies

---- SLOT [7] ----
Shared IPv6 Mcast Adjacencies Index  Packets      Bytes
---------------------------- ------ ------------ ------------------
Subnet bridge adjacency      0x7F802 0           0
Control bridge adjacency     0x7     0           0
StarG_M bridge adjacency     0x8     0           0
S_G bridge adjacency         0x9     0           0
Default drop adjacency       0xA     0           0
StarG (spt == INF) adjacency 0xB     0           0
StarG (spt != INF) adjacency 0xC     0           0
```

This example shows how to display the IPv6-multicast statistics information:

```
Router# show platform software ipv6-multicast statistics
IPv6 Multicast HW-switching Status          : Enabled
IPv6 Multicast (*,G) HW-switching Status    : Disabled
IPv6 Multicast Subnet-entries Status        : Enabled
Default MFIB IPv6-table                      : 0x5108F770
(S,G,C) flowmask index                       : 3
(*,G,C) flowmask index                       : 65535
General Counters
--------------------------------------------------+------+
Mfib-hw-entries count                        0
Mfib-add count                               4
Mfib-modify count                            2
Mfib-delete count                            2
Mfib-NP-entries count                        0
Mfib-D-entries count                         0
Mfib-IC-entries count                        0
Error Counters
--------------------------------------------------+------+
ACL flowmask err count                       0
ACL TCAM exptn count                         0
```

```
ACL renable count                                       0
Idb Null error                                          0
```
This example shows how to display the IPv6-multicast hardware shortcut count:

```
Router# show platform software ipv6-multicast summary
IPv6 Multicast Netflow SC summary on Slot[7]:
Shortcut Type           Shortcut count
--------------------------+--------------
(S, G)                    0
IPv6 Multicast FIB SC summary on Slot[7]:
Shortcut Type           Shortcut count
--------------------------+--------------
(*, G/128)                0
(*, G/m)                  0
```

Related Commands

Command	Description
ipv6 mfib hardware-switching	Configures hardware switching for IPv6 multicast packets on a global basis.

show platform software vpn

To display information about the platform software for IPv6 Virtual Private Networks (VPNs), use the **show platform software vpn** command in privileged EXEC mode.

show platform software vpn [**status**| **mapping ios**]

Syntax Description

status	(Optional) Displays the VPN status.
mapping ios	(Optional) Displays the Cisco IOS mapping information.

Command Modes Privileged EXEC

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.

Usage Guidelines If no keyword is used, then all VPN information is displayed.

Examples The following example shows output regarding platform software for all VPNs:

```
Router# show platform software vpn
```

show tunnel 6rd

To display IPv6 rapid deployment (6RD) information about a tunnel, use the **show tunnel 6rd** command in privileged EXEC mode.

show tunnel 6rd [*tunnel-interface interface-number*]

Syntax Description

tunnel-interface(interface-number	(Optional) Specifies a tunnel interface and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **show tunnel 6rd** command displays 6RD-related information on a tunnel. If an interface is not specified, information about all the 6RD tunnels on the router is displayed.

Examples

The following is sample output from the show tunnel 6rd command:

```
Router# show tunnel 6rd tunnel 1
show tunnel 6rd tunnel 1
Interface Tunnel1:
  Tunnel Source: 10.1.2.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
      V4 Prefix, Length: 16, Value: 10.1.0.0
      V4 Suffix, Length: 8, Value: 0.0.0.1
  General Prefix: 2001:B000:200::/40
```

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

Table 43: show tunnel 6rd Field Descriptions

Field	Description
Interface Tunnel1:	The specified tunnel interface and number.
Tunnel Source: 10.1.2.1	The source address for the tunnel interface.
6RD: Operational	6RD is enabled on the router.
V6 Prefix: 2001:B000::/32	The common IPv6 prefix on IPv6 6RD tunnels.

Field	Description
V4 Common Prefix Length: 16, Value: 10.1.0.0	The prefix length and value of the IPv4 transport address common to all the 6RD routers in a domain.
V4 Common Suffix Length: 8, Value: 0.0.0.1	The suffix length and value of the IPv4 transport address common to all the 6RD routers in a domain.

Related Commands

Command	Description
tunnel 6rd prefix	Specifies the common IPv6 prefix on IPv6 6RD tunnels.
tunnel mode ipv6ip	Configures a static IPv6 tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

show tunnel 6rd destination

To translate an IPv6 rapid deployment (6RD) prefix to the corresponding IPv4 destination, use the **show tunnel 6rd destination**command in privileged EXEC mode.

show tunnel 6rd destination *ipv6-prefix tunnel-interface interface-number*

Syntax Description

ipv6-prefix	The IPv6 network assigned to the general prefix.
tunnel-interface interface-number	Specifies a tunnel interface and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **show tunnel 6rd destination** command is used to translate a 6RD prefix to the corresponding IPv4 destination. The IPv4 destination address is displayed in the command output.

Examples

The following is sample output from the **show tunnel 6rd destination** command:

```
Router# show tunnel 6rd destination 2001:B000:300:: tunnel 1

Interface: Tunnel1
6RD Prefix: 2001:B000:300::
Destination: 10.1.3.1.
```

Table 44: show tunnel 6rd destination Field Descriptions

Field	Description
Interface Tunnel1:	The specified tunnel interface and number.
6RD Prefix	The specified 6RD IPv6 prefix.
Destination: 10.1.3.1	The corresponding IPv4 destination.

Related Commands

Command	Description
tunnel 6rd prefix	Specifies the common IPv6 prefix on IPv6 6RD tunnels.
tunnel mode ipv6ip	Configures a static IPv6 tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

show tunnel 6rd prefix

To translate an IPv4 destination address to the corresponding IPv6 6RD prefix, use the **show tunnel 6rd prefix** command in privileged EXEC mode.

show tunnel 6rd prefix *ipv4-destination tunnel-interface interface-number*

Syntax Description

ipv4-destination	The IPv4 destination address.
tunnel-interface interface-number	Specifies a tunnel interface and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show tunnel 6rd prefix** command translates an IPv4 destination address to the corresponding IPv6 6RD prefix. The command output displays the 6rd prefix.

Examples

The following is sample output from the **show tunnel 6rd prefix** command:

```
Router# show tunnel 6rd prefix 10.1.3.1 tunnel 0

Interface: Tunnel0
Destination: 10.1.3.1
6RD Prefix: 2001:B000:300::
```

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

Table 45: show tunnel 6rd prefix Field Descriptions

Field	Description
Interface Tunnel0:	The specified tunnel interface and number.
Destination: 10.1.3.1	The IPv4 destination address.
6RD Prefix: 2001:B000:300::	The corresponding 6RD prefix.

Related Commands

Command	Description
tunnel 6rd prefix	Specifies the common IPv6 prefix on IPv6 6RD tunnels.
tunnel mode ipv6ip	Configures a static IPv6 tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

sip address

To configure a Session Initiation Protocol (SIP) server IPv6 address to be returned in the SIP server's IPv6 address list option to clients, use the **sip address**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip address *ipv6-address*

no sip address *ipv6-address*

Syntax Description

ipv6-address	An IPv6 address. The *ipv6-address* 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   No default behavior or values

Command Modes   DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines   For the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

The **sip address** command configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients. To configure multiple SIP server addresses, issue this command multiple times. The new addresses will not overwrite old ones.

Examples   In the following example, the SIP server IPv6 address 2001:0db8::2 is configured to be returned in the SIP server's IPv6 address list option to clients:

```
sip address 2001:0DB8::2
```

Related Commands

Command	Description
prefix-delegation aaa	Specifies that prefixes are to be acquired from AAA servers.
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

sip domain-name

To configure a Session Initiation Protocol (SIP) server domain name to be returned in the SIP server's domain name list option to clients, use the **sip domain-name**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip domain-name *domain-name*

no sip domain-name *domain-name*

Syntax Description

domain-name	A domain name for a DHCP for IPv6 client.

Command Default   No default behavior or values.

Command Modes   DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines   In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

The **sip domain-name** command configures a SIP server domain name to be returned in the SIP server's domain name list option to clients. To configure multiple SIP server domain names, issue this command multiple times. The new domain names will not overwrite old ones.

Examples   The following example configures the SIP server domain name sip1.cisco.com to be returned in the SIP server's domain name list option to clients:

```
sip domain-name sip1.cisco.com
```

Related Commands

Command	Description
prefix-delegation aaa	Specifies that prefixes are to be acquired from AAA servers.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients.

sip domain-name