IPv6 Commands: show ipv6 na to show ipv6 pr

show ipv6 nat statistics

To display Network Address Translation--Protocol Translation (NAT-PT) statistics, use the **show iv6 nat statistics**command in user EXEC or privileged EXEC mode.

show ipv6 nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

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

```
Router# show ipv6 nat statistics
Total active translations: 4 (2 static, 2 dynamic; 2 extended)
NAT-PT interfaces:
  Ethernet3/1, Ethernet3/3
Hits: 1  Misses: 1
Expired translations: 0
```

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

Table 1: show ipv6 nat statistics Field Descriptions

Field	Description
Total active translations	Number of translations active in the system. This number increments by one each time a translation is created and is decremented each time a translation is cleared or times out. Displays the numbers for each type of translation.
NAT-PT interfaces	The interfaces, by type and number, that are configured to run NAT-PT translations.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
Expired translations	Cumulative count of translations that have expired since the router was booted.

Related Commands

Command	Description
show ipv6 nat translations	Displays active NAT-PT translations.

show ipv6 nat translations

To display active Network Address Translation--Protocol Translation (NAT-PT) translations, use the **show ip nat translations** command in user EXEC or privileged EXEC mode.

show ipv6 nat translations [{**icmp** | **tcp** | **udp**}] [**verbose**]

Syntax Description		
icmp	(Optional) Displays detailed information about NAT-PT ICMP translation events.
tcp	(Optional) Displays detailed information about NAT-PT TCP translation events.
udp	(Optional) Displays detailed information about NAT-PT User Datagram Protocol (UDP) translation events.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following is sample output from the **show ip nat translations** command. Two static translations have been configured between an IPv4 source address and an IPv6 destination, and vice versa.

```
Router# show ipv6 nat translations
Prot  IPv4 source            IPv6 source
      IPv4 destination       IPv6 destination
---   ---                    ---
      192.168.123.2          2001::2
---   ---                    ---
      192.168.122.10         2001::10
tcp   192.168.124.8,11047    3002::8,11047
      192.168.123.2,23       2001::2,23
udp   192.168.124.8,52922    3002::8,52922
      192.168.123.2,69       2001::2,69
udp   192.168.124.8,52922    3002::8,52922
      192.168.123.2,52922    2001::2,52922
---   192.168.124.8          3002::8
      192.168.123.2          2001::2
---   192.168.124.8          3002::8
      ---                    ---
---   192.168.121.4          5001::4
      ---                    ---
```

The following is sample output that includes the **verbose** keyword:

```
Router# show ipv6 nat translations verbose
Prot  IPv4 source            IPv6 source
      IPv4 destination       IPv6 destination
```

```
---    ---                     ---
       192.168.123.2           2001::2
       create 00:04:24, use 00:03:24,
---    ---                     ---
       192.168.122.10          2001::10
       create 00:04:24, use 00:04:24,
tcp    192.168.124.8,11047     3002::8,11047
       192.168.123.2,23        2001::2,23
       create 00:03:24, use 00:03:20, left 00:16:39,
udp    192.168.124.8,52922     3002::8,52922
       192.168.123.2,69        2001::2,69
       create 00:02:51, use 00:02:37, left 00:17:22,
udp    192.168.124.8,52922     3002::8,52922
       192.168.123.2,52922     2001::2,52922
       create 00:02:48, use 00:02:30, left 00:17:29,
---    192.168.124.8           3002::8
       192.168.123.2           2001::2
       create 00:03:24, use 00:02:34, left 00:17:25,
---    192.168.124.8           3002::8
       ---                     ---
       create 00:04:24, use 00:03:24,
---    192.168.121.4           5001::4
       ---                     ---
       create 00:04:25, use 00:04:25,
```

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

Table 2: show ipv6 nat translations Field Descriptions

Field	Description
Prot	Protocol of the port identifying the address.
IPv4 source/IPv6 source	The IPv4 or IPv6 source address to be translated.
IPv4 destination/IPv6 destination	The IPv4 or IPv6 destination address.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
left	Time before the entry times out (in hours:minutes:seconds).

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation state table.

show ipv6 nd destination

To display information about IPv6 host-mode destination cache entries, use the **show ipv6 nd destination** command in user EXEC or privileged EXEC mode.

show ipv6 nd destination [**vrf** *vrf-name*] [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface- type	(Optional) Specifies the Interface type.
interface- number	(Optional) Specifies the Interface number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SE	This command was introduced.

Usage Guidelines

Use the **show ipv6 nd destination** command to display information about IPv6 host-mode destination cache entries. If the **vrf** *vrf-name* keyword and argument pair is used, then only information about the specified VRF is displayed. If the *interface-type* and *interface-number* arguments are used, then only information about the specified interface is displayed.

Examples

```
Device# show ipv6 nd destination

IPv6 ND destination cache (table: default)
Code: R - Redirect
   2001::1 [8]
    via FE80::A8BB:CCFF:FE00:5B00/Ethernet0/0
```

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

Table 3: show ipv6 nd destination Field Descriptions

Field	Description
Code: R - Redirect	Destinations learned through redirect.
2001::1 [8]	The value displayed in brackets is the time, in seconds, since the destination cache entry was last used.

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

show ipv6 nd on-link prefix

To display information about on-link prefixes learned through router advertisements (RAs), use the **show ipv6 nd on-link prefix** command in user EXEC or privileged EXEC mode.

show ipv6 nd on-link prefix [**vrf** *vrf-name*] [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface -type	(Optional) Specifies the Interface type.
interface -number	(Optional) Specifies the Interface number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SE	This command was introduced.

Usage Guidelines

Use the **show ipv6 nd on-link prefix** command to display information about on-link prefixes learned through RAs.

Prefixes learned from an RA may be inspected using the **show ipv6 nd on-link prefix** command. If the **vrf** *vrf-name* keyword and argument pair is used, then only information about the specified VRF is displayed. If the *interface-type* and *interface-number* arguments are used, then only information about the specified interface is displayed.

Examples

The following example displays information about on-link prefixes learned through RAs:

```
Device# show ipv6 nd on-link prefix

IPv6 ND on-link Prefix (table: default), 2 prefixes
Code: A - Autonomous Address Config
A  2001::/64  [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
2001:1:2::/64  [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
```

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

show ipv6 nd raguard counters

To display information about RA guard counters, use the **show ipv6 nd raguard policy**command in privileged EXEC mode.

show ipv6 nd raguard counters [**interface** *type number*]

Syntax Description	**interface** *type number*	(Optional) Displays RA guard policy information for the specified interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(5th)SXI	This command was introduced.

Usage Guidelines   The **show ipv6 nd raguard counters** command displays information about RA guard counters, such as packets sent, packets received, and packets droped. This command also provides information on why a packet was dropped.

show ipv6 nd raguard policy

To display a router advertisements (RAs) guard policy on all interfaces configured with the RA guard feature, use the **show ipv6 nd raguard policy** command in privileged EXEC mode.

show ipv6 nd raguard policy [*policy-name*]

Syntax Description

policy-name	(Optional) RA guard policy name.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show ipv6 nd raguard policy** command displays the options configured for the policy on all interfaces configured with the RA guard feature.

Examples

The following example shows the policy configuration for a policy named raguard1 and all the interfaces where the policy is applied:

```
Router# show ipv6 nd raguard policy interface raguard1

Policy raguard1 configuration:
  device-role host
Policy applied on the following interfaces:
  Et0/0        vlan all
  Et1/0        vlan all
```

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

Table 4: show ipv6 nd raguard policy Field Descriptions

Field	Description
Policy raguard1 configuration:	Configuration of the specified policy.
device-role host	The role of the device attached to the port. This device configuration is that of host.
Policy applied on the following interfaces:	The specified interface on which the RA guard feature is configured.

show ipv6 nd secured certificates

To display active IPv6 Secure Neighbor Discovery (SeND) certificates, use the **show ipv6 nd secured certificates**command in privileged EXEC mode.

show ipv6 nd secured certificates

Syntax Description

This command has no arguments or keywords.

Command Default

No SeND certificates are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured certificates** command is used on hosts (routers configured in host mode) to display the certifcates received over SeND (via Certificate Path Advertisement) and their state.

Examples

The following example displays active SeND certificates:

```
Router# show ipv6 nd secured certificates
Total number of entries: 1 / 32
Hash                            id        RA  certcnt certrcv state
DC0102E09FAF422D49ED79A846D2EBC1 0x00000778 no  1        1       CERT_VALIDATED
certificate No 0
subject  hostname=sa14-72a,c=FR,st=fr,l=example,o=cisco,ou=nsstg,cn=72a
```

issuer c=FR,st=fr,l=example,o=cisco,ou=nsstg,cn=CA0

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

Table 5: show ipv6 nd secured certificates Field Descriptions

Field	Description
certcnt	Number of certificate for this chain.
certrcv	Number of certifciate received in the chain.
Hash	Key hash.
id	Numero of the certifciate.
RA	Displays Yes if an RA is pending for this certifciate.
state	Current state of the certificate.

Related Commands

Command	Description
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 nd secured counters interface

To display IPv6 Secure Neighbor Discovery (SeND) counters on an interface, use the **show ipv6 nd secured counters interface**command in privileged EXEC mode.

show ipv6 nd secured counters interface *interface*

Syntax Description

interface	(Optional) Specifies the interface on which SeND counters are located.

Command Default

No SeND counter information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example displays SeND counters:

```
Router# show ipv6 nd secured counters interface ethernet0/0
e0/0 Received ND messages on Ethernet0/0:
rcvd    accept  SLLA    TLLA    PREFIX  MTU    CGA    RSA    TS     NONCE   TA CERT
RA      66      65      63      0       62     63     63     63     63      0      0
        0
NS      8       8       8       0       0      0      8      8      8       8      0
        0
NA      20      20      0       8       0      0      19     19     19      14     0
        0
CPA     1       1       0       0       0      0      0      0      0       0      1
        1
Dropped ND messages on Ethernet0/0:
Codes   TIMEOUT: Timed out while waiting for rsp
        drop    TIMEOUT
RA      1       1
Sent ND messages on Ethernet0/0:
sent    aborted SLLA    CGA     RSA     TS     NONCE   TA
NS      14      0       14      14      14     14      14     0
NA      8       0       0       8       8      8       8      0
CPS     43      0       0       0       0      0       0      43
Router#
```

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

Table 6: show ipv6 nd secured counters interface Field Descriptions

Field	Description
accept	Number of neighbor discovery (ND) messages accepted (messages that are not dropped).
CERT	Number of messages received with the certificate option.
CGA	Number of messages received with the CGA option.

Field	Description
MTU	Number of messages received with the MTU option.
NA	Number of NDP neighbor advertisements
NONCE	Number of messages received with the NONCE option.
NS	Number of NDP neighbor solicitions.
PREFIX	Number of messages received with the PREFIX option.
rcvd	Number of ND messages received on the interface.
RA	Number of router advertisements.
REDIR	Number of NDP redirect messages.
RS	Router Solicit.
RSA	Number of messages received with the RSA option.
SLLA	Number of messages received with the ND SLLA option.
TA	Number of messages received with the trust anchor option.
TS	Number of messages received with the time stamp option.

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND timestamp entries.

show ipv6 nd secured nonce-db

To display active IPv6 Secure Neighbor Discovery (SeND) nonce database entries, use the **show ipv6 nd secured nonce-db**command in privileged EXEC mode.

show ipv6 nd secured nonce-db

Syntax Description	This command has no arguments or keywords.
Command Default	No SeND nonce information is displayed.
Command Modes	Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured nonce-db**command is used to display the pending solicitations. There are rarely any pending solicitations because the solicitations are quickly answered and removed from the database.

Examples

The following example displays active SeND nonce entries. The output is self-explanatory.

```
Router# show ipv6 nd secured nonce-db
Total number of entries: 0
```

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured timestamp-db	Displays active SeND time stamp entries.

show ipv6 nd secured solicit-db

To display pending SEcure Neighbor Discovery (SEND) solicitations from peers, use the **show ipv6 nd secured solicit-db**command in privileged EXEC configuration mode.

show ipv6 nd secured solicit-db

Syntax Description This command has no arguments or keywords.

Command Default No pending SEND solicitation information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines Use this command to display pending SEND solicitations.

Examples The following example displays pending SEcure Neighbor Discovery (SEND) solicitations from peers:

```
Router# show ipv6 nd secured solicit-db
```

show ipv6 nd secured timestamp-db

To display active Secure Neighbor Discovery (SeND) time-stamp database entries, use the **show ipv6 nd secured timestamp-db**command in privileged EXEC mode.

show ipv6 nd secured timestamp-db

Syntax Description	This command has no arguments or keywords.
Command Default	No pending SeND solicitation information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured timestamp-db** command displays the content of the time-stamp databse, which contains last received messages from peers. It also displays the delta and fuzz values.

Examples

The following example displays active SeND time-stamp database entries:

```
Router# show ipv6 nd secured timestamp-db
Total number of entries: 6 Number of unreached peer entries: 3 / 1024
FE80::289C:3308:4719:87F2 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 41m 16s (reached)
        TSlast: 0x4936B97655FF = Wed Dec  3 16:53:10 2008
        RDlast: 0x4936B976438B = Wed Dec  3 16:53:10 2008
FE80::2441:88D1:22FC:3B77 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 59m 53s (reached)
        TSlast: 0x4936BDD2E13E = Wed Dec  3 17:11:46 2008
        RDlast: 0x4936BDD2D0D6 = Wed Dec  3 17:11:46 2008
FE80::E2:F012:6F72:9E45 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 18s (unreached)
        TSlast: 0x4936B0CBB333 = Wed Dec  3 16:16:11 2008
        RDlast: 0x4936B0CBBD70 = Wed Dec  3 16:16:11 2008 2001:100::38C9:4A1A:2972:794E on
 Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 19s (unreached)
        TSlast: 0x4936BA254FDA = Wed Dec  3 16:56:05 2008
        RDlast: 0x4936BA253F72 = Wed Dec  3 16:56:05 2008 2001:100::383E:6BD5:397:4A50 on
Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 45m 0s (reached)
        TSlast: 0x4936BA55F2AA = Wed Dec  3 16:56:53 2008
        RDlast: 0x4936BA55E036 = Wed Dec  3 16:56:53 2008
2001:100::434:E62D:327D:B1E6 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 42s (unreached)
        TSlast: 0x4936B0E422D0 = Wed Dec  3 16:16:36 2008
        RDlast: 0x4936B0E42D0E = Wed Dec  3 16:16:36 2008
```

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

Table 7: show ipv6 nd secured timestamp-db Field Descriptions

Field	Description
Total number of entries	Number of entries (peers) in the cache.
Time to expire	Remaining time before entry expires.
TSlast	Last peer timestamp value.
RDlast	Time when the last message was received from the peer.

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.

show ipv6 neighbor binding

To display contents of a binding table, use the **show ipv6 neighbor binding** command in privileged EXEC mode.

show ipv6 neighbor binding [{**vlan** *vlan-id* | **interface** *type number* | **ipv6** *ipv6-address* | **mac** *mac-address*}]

Syntax Description

vlan *vlan-id*	(Optional) Displays the binding table entries that match the specified VLAN.
interface *type number*	(Optional) Displays the binding table entries that match the specified interface type and number.
ipv6 *ipv6-address*	(Optional) Displays the binding table entries that match the specified IPv6 address.
mac *mac-address*	(Optional) Displays the binding table entries that match the specified Media Access Control (MAC) address.

Command Modes

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 neighbor binding** command displays the contents of the binding table. The display output can be specified by the specified VLAN, interface, IPv6 address, or MAC address. If no keywords or arguments are entered, all binding table contents are displayed.

The following keyword and argument combinations are allowed:

- **vlan** *vlan-id*: Displays all entries for the specified VLAN.

- **interface** *type number*: Displays all entries for the specified interface.

- **ipv6** *ipv6-address* + **interface** *type number* + **vlan** *vlan-id*: Displays a single entry that matches these three keyword and argument combinations.

- **ipv6** *ipv6-address* + **interface** *type number*: Displays all entries for the specified IPv6 address and interface.

- **ipv6** *ipv6-address*: Displays all entries for the specified IPv6 address.

Examples

The following example displays the contents of a binding table:

```
Device# show ipv6 neighbor binding

address DB has 4 entries
Codes: L - Local, S - Static, ND - Neighbor Discovery
Preflevel (prlvl) values:
1:Not secure          2:MAC and LLA match   3:Cga authenticated
4:Dhcp assigned       5:Cert authenticated  6:Cga and Cert auth
7:Trusted port        8:Statically assigned
     IPv6 address          Link-Layer addr Interface   vlan  prlvl age state    Time left
ND  FE80::A8BB:CCFF:FE01:F500  AABB.CC01.F500  Et0/0      100  0002    0 REACHABLE 8850
L   FE80::21D:71FF:FE99:4900   001D.7199.4900  Vl100      100  0080 7203 DOWN      N/A
ND  2001:600::1               AABB.CC01.F500  Et0/0      100  0003    0 REACHABLE 3181
ND  2001:300::1               AABB.CC01.F500  Et0/0      100  0007    0 REACHABLE 9559
ND  2001:100::2               AABB.CC01.F600  Et1/0      200  0002    0 REACHABLE 9196
L   2001:400::1               001D.7199.4900  Vl100      100  0080 7188 DOWN      N/A
S   2001:500::1               000A.000B.000C  Fa4/13     300  0080 8676 STALE     N/A
```

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

Table 8: show ipv6 neighbor binding Field Descriptions

Field	Description
address DB has *n* entries	Number of entries in the specified database.

Related Commands	**Command**	**Description**
	ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

show ipv6 neighbors

To display IPv6 neighbor discovery (ND) cache information, use the **show ipv6 neighbors** command in user EXEC or privileged EXEC mode.

show ipv6 neighbors [{*interface-type interface-numberipv6-addressipv6-hostname* | **statistics**}]

Syntax Description		
interface-type	(Optional) Specifies the type of the interface from which IPv6 neighbor information is to be displayed.	
interface-number	(Optional) Specifies the number of the interface from which IPv6 neighbor information is to be displayed.	
ipv6-address	(Optional) Specifies the 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.	
ipv6-hostname	(Optional) Specifies the IPv6 hostname of the remote networking device.	
statistics	(Optional) Displays ND cache statistics.	

Command Default All IPv6 ND cache entries are listed.

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. Support for static entries in the IPv6 neighbor discovery cache was added to 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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and introduced on Cisco ASR 1000 Series devices.

Release	Modification
Cisco IOS XE Release 2.6	This command was modified. This command was updated to display the number and the limit of ND cache entries on a particular interface.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.
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

When the *interface-type* and *interface-number* arguments are not specified, cache information for all IPv6 neighbors is displayed. Specifying the *interface-type* and *interface-number* arguments displays only cache information about the specified interface.

Specifying the **statistics** keyword displays ND cache statistics.

The following is sample output from the **show ipv6 neighbors** command when entered with an interface type and number:

```
Device# show ipv6 neighbors ethernet 2
IPv6 Address                            Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e  REACH Ethernet2
FE80::203:A0FF:FED6:141E                  0 0003.a0d6.141e  REACH Ethernet2
3001:1::45a                               - 0002.7d1a.9472  REACH Ethernet2
```

The following is sample output from the **show ipv6 neighbors** command when entered with an IPv6 address:

```
Device# show ipv6 neighbors 2000:0:0:4::2
IPv6 Address                            Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e  REACH Ethernet2
```

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

Table 9: show ipv6 neighbors Field Descriptions

Field	Description
IPv6 Address	IPv6 address of neighbor or interface.
Age	Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
Link-layer Addr	MAC address. If the address is unknown, a hyphen (-) is displayed.

Field	Description
State	The state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache: • INCMP (Incomplete)--Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received. • REACH (Reachable)--Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent. • STALE--More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • DELAY--More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE. • PROBE--A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received. • ????--Unknown state. Following are the possible states for static entries in the IPv6 neighbor discovery cache: • INCMP (Incomplete)--The interface for this entry is down. • REACH (Reachable)--The interface for this entry is up. **Note** Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (Incomplete) and REACH (Reachable) states are different for dynamic and static cache entries.
Interface	Interface from which the address was reachable.

The following is sample output from the **show ipv6 neighbors** command with the **statistics** keyword:

```
Device# show ipv6 neighbor statistics

IPv6 ND Statistics
 Entries 2, High-water 2, Gleaned 1, Scavenged 0
 Entry States
   INCMP 0  REACH 0  STALE 2  GLEAN 0  DELAY 0  PROBE 0
 Resolutions (INCMP)
   Requested 1, timeouts 0, resolved 1, failed 0
   In-progress 0, High-water 1, Throttled 0, Data discards 0
 Resolutions (PROBE)
   Requested 3, timeouts 0, resolved 3, failed 0
```

The table below describes the significant fields shown in this display:

Table 10: show ipv6 neighbors statistics Field Descriptions

Field	Description
Entries	Total number of ND neighbor entries in the ND cache.
High-Water	Maximum amount (so far) of ND neighbor entries in ND cache.
Gleaned	Number of ND neighbor entries gleaned (that is, learned from a neighbor NA or other ND packet).
Scavenged	Number of stale ND neighbor entries that have timed out and been removed from the cache.
Entry States	Number of ND neighbor entries in each state.
Resolutions (INCMP)	Statistics for neighbor resolutions attempted in INCMP state (that is, resolutions prompted by a data packet). Details about the resolutions attempted in INCMP state are follows: • Requested--Total number of resolutions requested. • Timeouts--Number of timeouts during resolutions. • Resolved--Number of successful resolutions. • Failed--Number of unsuccessful resolutions. • In-progress--Number of resolutions in progress. • High-water--Maximum number (so far) of resolutions in progress. • Throttled--Number of times resolution request was ignored due to maximum number of resolutions in progress limit. • Data discards--Number of data packets discarded that are awaiting neighbor resolution.
Resolutions (PROBE)	Statistics for neighbor resolutions attempted in PROBE state (that is, re-resolutions of existing entries prompted by a data packet): • Requested--Total number of resolutions requested. • Timeouts--Number of timeouts during resolutions. • Resolved--Number of successful resolutions. • Failed--Number of unsuccessful resolutions.

show ipv6 nhrp

To display Next Hop Resolution Protocol (NHRP) mapping information, use the **show ipv6 nhrp** command in user EXEC or privileged EXEC mode.

show ipv6 nhrp [{**dynamic** [*ipv6-address*] | **incomplete** | **static**}] [{**address** | **interface**}] [{**brief** | **detail**}] [**purge**]

Syntax Description

dynamic	(Optional) Displays dynamic (learned) IPv6-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See the table below for types, number ranges, and descriptions.
ipv6-address	(Optional) The IPv6 address of the cache entry.
incomplete	(Optional) Displays information about NHRP mapping entries for which the IPv6-to-NBMA is not resolved. See the table below for types, number ranges, and descriptions.
static	(Optional) Displays static IPv6-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the **ipv6 nhrp map** command. See the table below for types, number ranges, and descriptions.
address	(Optional) NHRP mapping entry for specified protocol addresses.
interface	(Optional) NHRP mapping entry for the specified interface. See the table below for types, number ranges, and descriptions.
brief	(Optional) Displays a short output of the NHRP mapping.
detail	(Optional) Displays detailed information about NHRP mapping.
purge	(Optional) Displays NHRP purge information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 11: Valid Types, Number Ranges, and Interface Description

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

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

```
Router# show ipv6 nhrp
2001:0db8:3c4d:0015::1a2f:3d2c/48  via
2001:0db8:3c4d:0015::1a2f:3d2c
Tunnel0 created 6d05h, never expire
```

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

Table 12: show ipv6 nhrp Field Descriptions

Field	Description
2001:0db8:3c4d:0015::1a2f: 3d2c/48	Target network.
2001:0db8:3c4d:0015::1a2f:3d2c	Next hop to reach the target network.
Tunnel0	Interface through which the target network is reached.
created 6d05h	Length of time since the entry was created (dayshours).
never expire	Indicates that static entries never expire.

The following is sample output from the **show ipv6 nhrp**command using the **brief** keyword:

```
Router# show ipv6 nhrp brief
2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/48
 via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c
Interface: Tunnel0 Type: static
NBMA address: 10.11.11.99
```

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

Table 13: show ipv6 nhrp brief Field Descriptions

Field	Description
2001:0db8:3c4d:0015:0000:0000: 1a2f:3d2c/48	Target network.
via 2001:0db8:3c4d:0015:0000:0000: 1a2f:3d2c	Next Hop to reach the target network.
Interface: Tunnel0	Interface through which the target network is reached.
Type: static	Type of tunnel. The types can be one of the following: • dynamic--NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations. • static--NHRP mapping is configured statically. Entries configured by the **ipv6 nhrp map** command are marked static. • incomplete--The NBMA address is not known for the target network.

Related Commands	Command	Description
	ipv6 nhrp map	Statically configures the IPv6-to-NBMA address mapping of IP destinations connected to an NBMA network.

show ipv6 nhrp multicast

To display Next Hop Resolution Protocol (NHRP) multicast mapping information, use the **show ipv6 nhrp multicast**command in user EXEC or privileged EXEC mode.

show ipv6 nhrp multicast [{**ipv4-address** | **interface***ipv6-address*}]

Syntax Description

ipv4-address	(Optional) The IPv4 address of the multicast mapping entry.
interface	(Optional) All multicast mapping entries of the NHRP network for the interface. See the table below for interface types, number ranges, and descriptions.
ipv6-address	(Optional) The IPv6 address of the multicast mapping entry.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.2(1)T	This command was modified. The *ipv4-address* argument was added.

Usage Guidelines

The table below lists valid interface types, number ranges, and descriptions for the optional *interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 14: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex

Valid Types	Number Ranges	Interface Descriptions
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ipv6 nhrp multicast** command. Fields in the display are self-explanatory.

```
Router# show ipv6 nhrp multicast
  I/F     NBMA address
Tunnel1    192.169.2.10     Flags: dynamic
Tunnel1    192.169.2.11     Flags: dynamic
```

Related Commands

Command	Description
ipv6 nhrp map	Statically configures the IPv6-to-NBMA address mapping of IPv6 destinations connected to an NBMA network.

show ipv6 nhrp multicast stats

To display multicast mapping statistics for one or all interfaces, use the **show ipv6 nhrp multicast stats** command in Privileged EXEC mode. The command displays statistics such as the count of enqueued, dequeued, and dropped packets.

show ipv6 nhrp multicast [*interface-name*] **stats**

Syntax Description

interface-name	Displays multicast mapping statistics for the specified interface.
	Example: **show ipv6 nhrp multicast tunnel0 stats**

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.8.1	Command introduced.

Example

```
SPOKE1#show ipv6 nhrp multicast stats
Legend: (m/n) - (m packets/n milliseconds)
==========================================================================================

Global stats
Total multicast pkts enqueued      4
Total multicast failed to enqueue 0
Total multicast pkts dequeued      4
Invalid multicast pkts dequeued    0
Total multicast pkts dropped       0

Interface stats
                             Enqueued/Failed        Dequeued/Rep fail      Dropped
                          -------------------------  -------------------------  ----------
   Tu0    (250   /    10)            4/0                       4/0                      0
```

show ipv6 nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ipv6 nhrp nhs** command in user EXEC or privileged EXEC mode.

show ipv6 nhrp nhs [*interface-type interface-number*] [{**detail** | **redundancy**}] [{**cluster** *number* | **preempted** | **running** | **waiting**}]

<table>
<tr><td rowspan="8">**Syntax Description**</td><td>*interface-type*</td><td>(Optional) Type of interface for which NHS information should be displayed. See the table below for types, number ranges, and descriptions.</td></tr>
<tr><td>*interface-number*</td><td>(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.</td></tr>
<tr><td>**detail**</td><td>(Optional) Displays detailed NHS information.</td></tr>
<tr><td>**redundancy**</td><td>(Optional) Displays NHS recovery information.</td></tr>
<tr><td>**cluster** *number*</td><td>(Optional) Displays NHS recovery cluster information. The range is from 0 to 10.</td></tr>
<tr><td>**preempted**</td><td>(Optional) Displays NHSs that come up and are preempted.</td></tr>
<tr><td>**running**</td><td>(Optional) Displays NHSs that are responding or expecting replies.</td></tr>
<tr><td>**waiting**</td><td>(Optional) Displays NHSs that are waiting to be scheduled.</td></tr>
</table>

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.1(2)T	This command was modified. The **redundancy**, **cluster** *number*, **preempted**, **running**, and **waiting** keywords and argument were added.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface-interface* argument.

✎

Note   The valid types can vary according to the platform and interfaces on the platform.

Table 15: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async

Valid Types	Number Ranges	Interface Descriptions
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	Fast Ethernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

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

```
Router# show ipv6 nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
192.0.2.1  W priority = 2 cluster = 0
192.0.2.2  RE priority = 0 cluster = 0
192.0.2.3  RE priority = 1 cluster = 0
```

The following is sample output from the **show ipv6 nhrp nhs redundancy** command:

```
Router# show ipv6 nhrp nhs redundancy
Legend: E=Expecting replies, R=Responding, W=Waiting
No.  Interface  Cluster  NHS        Priority  Cur-State  Cur-Queue  Prev-State  Prev-Queue
1    Tunnel0    5        2001::101  1         E          Running    RE          Running
```

```
No.  Interface  Cluster  Status   Max-Con  Total-NHS  Responding  Expecting  Waiting  Fallback
1    Tunnel0    5        Disable  Not Set  1          0           1          0        0
```

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

Table 16: show ipv6 nhrp nhs Field Descriptions

Field	Description
Tunnel0	Interface through which the target network is reached.
priority	Priority value assigned to the NHS.
cluster	Group to which the NHS belong.
E=Expecting replies	NHSs that are active and expecting replies.
R=Responding	NHSs that are active and responding.
W=Waiting	NHSs that are preempted and are not in the active probe list.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	Displays NHRP traffic statistics.

show ipv6 nhrp summary

To display Next Hop Resolution Protocol (NHRP) mapping summary information, use the **show ipv6 nhrp summary** command in user EXEC or privileged EXEC mode.

show ipv6 nhrp summary

Syntax Description
This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines
Use this command to monitor NHRP.

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

```
Router# show ipv6 nhrp summary
IPV6 NHRP cache 1 entry, 256 bytes
    1 static  0 dynamic  0 incomplete
```

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

Table 17: show ipv6 nhrp summary Field Descriptions

Field Output	Description
static	NHRP mapping is configured statically. Entries configured by the **ipv6 nhrp map** command are marked static.
dynamic	NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations
incomplete	The nonbroadcast multiaccess (NBMA) address is not known for the target network.

Related Commands

Command	Description
ip nhrp map	Statically configures the IPv6-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ipv6 nhrp	Displays NHRP mapping information.

show ipv6 nhrp traffic

To display Next Hop Resolution Protocol (NHRP) traffic statistics, use the **show ipv6 nhrp traffic** command in privileged EXEC mode.

show ipv6 nhrp traffic [{**throttled** | **interface**{**tunnel** *number* | **Virtual-Access** *number*}}]

Syntax Description

throttled	(Optional) Displays information about NHRP traffic that is throttled.
interface	(Optional) Displays NHRP traffic information for a given interface.
tunnel *number*	(Optional) Specifies the tunnel interface number.
Virtual-Access *number*	Specifies the virtual access interface number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.3(2)T	This command was modified. The **Virtual-Access** *number* keyword-argument pair was added.
Cisco IOS XE 16.3.2	This command was modified. The **throttled** keyword was added.

Usage Guidelines

Use this command to monitor NHRP traffic information.

Examples

The following example provides output for IPv6 NHRP traffic statistics:

```
Router# show ipv6 nhrp traffic
Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
Sent: Total 8
1 Resolution Request 1 Resolution Reply 6 Registration Request
0 Registration Reply 0 Purge Request 0 Purge Reply
0 Error Indication 0 Traffic Indication
Rcvd: Total 5
1 Resolution Request 1 Resolution Reply 0 Registration Request
2 Registration Reply 0 Purge Request 0 Purge Reply
0 Error Indication 1 Traffic Indication
```

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

Table 18: show ipv6 nhrp traffic Field Descriptions

Field Output	Description
tunnel0:	Displays information about a specified tunnel; in thhis case, Tunnel0.

Field Output	Description
Max-send limit: 100Pkts/10Sec, Usage: 0%	The maximum number of packets allowed to be sent in a specified time, and the current usage.
Sent: Total 8	Number of packets sent.
1 Resolution Request 1 Resolution Reply 6 Registration Request 0 Registration Reply 0 Purge Request 0 Purge Reply	Description and breakdown of of the types of packets sent.
0 Error Indication 0 Traffic Indication	Number of errors in the sent packets.
Rcvd: Total 5	Number of packets received.
1 Resolution Request 1 Resolution Reply 0 Registration Request 2 Registration Reply 0 Purge Request 0 Purge Reply	Description and breakdown of the types of packets received.
0 Error Indication 1 Traffic Indication	Number of errors in the sent packets.

show ipv6 ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ipv6 ospf** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] [**rate-limit**]

Syntax Description		
process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Area ID. This argument displays information about a specified area only.
rate-limit	(Optional) Rate-limited link-state advertisements (LSAs). This keyword displays LSAs that are currently being rate limited, together with the remaining time to the next generation.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	Command output is changed when authentication is enabled.
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.
12.4(9)T	Command output was updated to display OSPF for IPv6 encryption information.
12.4(15)XF	Command output was modified to include VMI PPPoE process-level values.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	The **rate-limit** keyword was added. Command output was modified to include the configuration values for SPF and LSA throttling timers.
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 integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.

Release	Modification
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Examples

show ipv6 ospf Output Example

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

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.10.10.1
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this device is 1. 1 normal 0 stub 0 nssa
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        MD5 Authentication, SPI 1000
        SPF algorithm executed 2 times
        Number of LSA 5. Checksum Sum 0x02A005
        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 19: show ipv6 ospf Field Descriptions

Field	Description
Routing process "ospfv3 1" with ID 10.10.10.1	Process ID and OSPF device ID.
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of areas	Number of areas in device, area addresses, and so on.

show ipv6 ospf With Area Encryption Example

The following sample output shows the **show ipv6 ospf** command with area encryption information:

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.0.0.1
It is an area border device
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this device is 2. 2 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        SPF algorithm executed 3 times
        Number of LSA 31. Checksum Sum 0x107493
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 20
        Flood list length 0
    Area 1
        Number of interfaces in this area is 2
        NULL Encryption SHA-1 Auth, SPI 1001
        SPF algorithm executed 7 times
        Number of LSA 20. Checksum Sum 0x095E6A
        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 20: show ipv6 ospf with Area Encryption Information Field Descriptions

Field	Description
Area 1	Subsequent fields describe area 1.
NULL Encryption SHA-1 Auth, SPI 1001	Displays the encryption algorithm (in this case, null, meaning no encryption algorithm is used), the authentication algorithm (SHA-1), and the security policy index (SPI) value (1001).

The following example displays the configuration values for SPF and LSA throttling timers:

```
Device# show ipv6 ospf
 Routing Process "ospfv3 1" with ID 10.9.4.1
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary device
 Redistributing External Routes from,
    ospf 2
 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
```

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

Table 21: show ipv6 ospf with SPF and LSA Throttling Timer Field Descriptions

Field	Description
Initial SPF schedule delay	Delay time of SPF calculations.
Minimum hold time between two consecutive SPFs	Minimum hold time between consecutive SPF calculations.
Maximum wait time between two consecutive SPFs 10000 msecs	Maximum hold time between consecutive SPF calculations.
Minimum LSA interval 5 secs	Minimum time interval (in seconds) between link-state advertisements.
Minimum LSA arrival 1000 msecs	Maximum arrival time (in milliseconds) of link-state advertisements.

The following example shows information about LSAs that are currently being rate limited:

```
Device# show ipv6 ospf rate-limit
List of LSAs that are in rate limit Queue
    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
```

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

Table 22: show ipv6 ospf rate-limit Field Descriptions

Field	Description
LSAID	Link-state ID of the LSA.
Type	Description of the LSA.
Adv Rtr	ID of the advertising device.
Due in:	Remaining time until the generation of the next event.

show ipv6 ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ipv6 ospf border-routers** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*] **border-routers**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show ipv6 ospf border-routers** command:

```
Router# show ipv6 ospf border-routers

OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

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

Table 23: show ipv6 ospf border-routers Field Descriptions

Field	Description
i - Intra-area route, I - Inter-area route	The type of this route.
172.16.4.4, 172.16.3.3	Router ID of the destination router.
[2], [1]	Metric used to reach the destination router.

Field	Description
FE80::205:5FFF:FED3:5808, FE80::205:5FFF:FED3:5406, FE80::205:5FFF:FED3:5808	Link-local routers.
FastEthernet0/0, POS4/0	The interface on which the IPv6 OSPF protocol is configured.
ABR	Area border router.
ASBR	Autonomous system boundary router.
Area 0, Area 1	The area ID of the area from which this route is learned.
SPF 13, SPF 8, SPF 3	The internal number of the shortest path first (SPF) calculation that installs this route.

show ipv6 ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the **show ipv6 ospf database** command in user EXEC or privileged EXEC mode. The various forms of this command deliver information about different OSPF link-state advertisements (LSAs).

show ipv6 ospf [*process-id* [*area-id*]] **database** [{**adv-router** *router-id* | **self-originate**}] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**database-summary**]

{**show ipv6 ospf** [*process-id* [*area-id*]] **database** [**external** [**ipv6-prefix**] [*link-state-id*]] | [{**adv-router** *router-id* | **self-originate**}] [**internal**]}

show ipv6 ospf [*process-id* [*area-id*]] **database** [**grace**]

{**show ipv6 ospf** [*process-id* [*area-id*]] **database** [**inter-area prefix** [**ipv6-prefix**] [*link-state-id*]] | [{**adv-router** *router-id* | **self-originate**}] [**internal**]}

{**show ipv6 ospf** [*process-id* [*area-id*]] **database** [**inter-area router** [**destination-router-id**] [*link-state-id*]] | [{**adv-router** *router-id* | **self-originate**}] [**internal**]}

show ipv6 ospf [*process-id* [*area-id*]] **database** [**link** [**interface** *interface-name*] [*link-state-id*]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**network** [*link-state-id*]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**nssa-external** [*ipv6-prefix*] [*link-state-id*]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**prefix** [**ref-lsa** {**router** | **network**}] [*link-state-id*]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**router** [*link-state-id*]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [{[{**router** | **network** | [{**external** *ipv6-prefix* | **nssa-external** *ipv6-prefix* | **inter-area** {**prefix** *ipv6-prefix* | **router**}}] | **link** | **prefix**}] | **database-summary**}] [{**adv-router** *router-id* | **self-originate**}] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**unknown** [{**area** | **as** | **link**} [*link-state-id*]]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]

Syntax Description		
process-id	(Optional) Displays information only about a specified process.
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.
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).
internal	(Optional) Internal LSA information.
database-summary	(Optional) Displays how many of each type of LSAs exist for each area in the database, and the total.
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.
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.
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.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
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	The **grace** keyword was added to show information about OSPFv3 graceful restart.

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 ipv6 ospf** database command to provide more detailed information.

Examples

The following is sample output from the **show ipv6 ospf database** command when no arguments or keywords are used:

```
Router# show ipv6 ospf 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 24: show ipv6 ospf 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.

Field	Description
Ref-lstype	Referenced link-state type.
Ref-LSID	Referenced link-state ID.

The following is sample output from the **show ipv6 ospf database** command with the **router self-originate** keywords:

```
Router# show ipv6 ospf database router self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Router Link States (Area 0)
 LS age: 383
 Options: (V6-Bit E-Bit R-bit DC-Bit)
 LS Type: Router Links
 Link State ID: 0
 Advertising Router: 172.16.6.6
 LS Seq Number: 80000003
 Checksum: 0x7543
 Length: 40
 Area Border Router
 Number of Links: 1
   Link connected to: another Router (point-to-point)
     Link Metric: 1
     Local Interface ID: 14
     Neighbor Interface ID: 14
     Neighbor Router ID: 172.16.4.4
```

The following is sample output from the **show ipv6 ospf database** command with the **network** keyword:

```
Router# show ipv6 ospf database network

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Net Link States (Area 1)
 LS age: 419
 Options: (V6-Bit E-Bit R-bit DC-Bit)
 LS Type: Network Links
 Link State ID: 3 (Interface ID of Designated Router)
 Advertising Router: 172.16.6.6
 LS Seq Number: 80000001
 Checksum: 0x8148
 Length: 32
       Attached Router: 172.16.6.6
       Attached Router: 172.16.3.3
```

The following is sample output from the **show ipv6 ospf database** command with the **link self-originate** keywords:

```
Router# show ipv6 ospf database link self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Link (Type-8) Link States (Area 0)
 LS age: 505
 Options: (V6-Bit E-Bit R-bit DC-Bit)
 LS Type: Link-LSA (Interface: POS4/0)
 Link State ID: 14 (Interface ID)
 Advertising Router: 172.16.6.6
 LS Seq Number: 80000002
```

```
        Checksum: 0xABF6
        Length: 60
        Router Priority: 1
        Link Local Address: FE80::205:5FFF:FED3:6408
        Number of Prefixes: 2
        Prefix Address: FEC0:4466::
        Prefix Length: 32, Options: None
        Prefix Address: FEC0:4466::
        Prefix Length: 32, Options: None
```

The following is sample output from the **show ipv6 ospf database** command with the **prefix self-originate**keywords:

```
Router# show ipv6 ospf database prefix self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Intra Area Prefix Link States (Area 0)
Routing Bit Set on this LSA
LS age: 552
LS Type: Intra-Area-Prefix-LSA
Link State ID: 0
Advertising Router: 172.16.6.6
LS Seq Number: 80000002
Checksum: 0xA910
Length: 48
Referenced LSA Type: 2001
Referenced Link State ID: 0
Referenced Advertising Router: 172.16.6.6
Number of Prefixes: 2
Prefix Address: FEC0:4466::
Prefix Length: 32, Options: None, Metric: 1
Prefix Address: FEC0:4466::
Prefix Length: 32, Options: None, Metric: 1
```

The following is sample output from the **show ipv6 ospf database** command with the **inter-area prefix self-originate**keywords:

```
Router# show ipv6 ospf database inter-area prefix self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Inter Area Prefix Link States (Area 0)
LS age: 587
LS Type: Inter Area Prefix Links
Link State ID: 0
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0x1395
Length: 32
Metric: 1
Prefix Address: FEC0:3366::
Prefix Length: 32, Options: None
LS age: 532
LS Type: Inter Area Prefix Links
Link State ID: 1
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0x3197
Length: 32
Metric: 2
Prefix Address: FEC0:3344::
Prefix Length: 32, Options: None
LS age: 422
LS Type: Inter Area Prefix Links
```

```
        Link State ID: 2
        Advertising Router: 172.16.6.6
        LS Seq Number: 80000001
        Checksum: 0xCB74
        Length: 32
        Metric: 1
        Prefix Address: FEC0::
        Prefix Length: 32, Options: None
```

The following is sample output from the **show ipv6 ospf database** command with the **inter-area router self-originate** keywords:

```
Router# show ipv6 ospf database inter-area router self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Inter Area Router Link States (Area 0)
  LS age: 578
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Inter Area Router Links
  Link State ID: 50529027
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000001
  Checksum: 0x369F
  Length: 32
  Metric: 1
  Destination Router ID: 172.16.3.3
```

The following is sample output from the **show ipv6 ospf database** command with the **external** keyword:

```
Router# show ipv6 ospf database external
            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Type-5 AS External Link States
  Routing Bit Set on this LSA
  LS age: 654
  LS Type: AS External Link
  Link State ID: 0
  Advertising Router: 172.16.3.3
  LS Seq Number: 80000001
  Checksum: 0x218D
  Length: 32
  Prefix Address: FEC0:3333::
  Prefix Length: 32, Options: None
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
```

The following is sample output from the **show ipv6 ospf database** command for a graceful-restart-capable router:

```
Router# show ipv6 ospf 1 database
            OSPFv3 Router with ID (10.2.2.2) (Process ID 1)
            Router Link States (Area 0)
ADV Router       Age         Seq#          Fragment ID  Link count  Bits
10.1.1.1         1949        0x8000000e         0            1       None
10.2.2.2         2007        0x80000011         0            1       None
            Link (Type-8) Link States (Area 0)
ADV Router       Age         Seq#          Link ID     Interface
10.1.1.1         180         0x80000006         1          PO0/2/0/0
10.2.2.2         2007        0x80000006         1          PO0/2/0/0
            Intra Area Prefix Link States (Area 0)
ADV Router       Age         Seq#          Link ID     Ref-lstype   Ref-LSID
10.1.1.1         180         0x80000006         0          0x2001        0
```

```
10.2.2.2         2007        0x80000006         0        0x2001          0
             Grace (Type-11) Link States (Area 0)
ADV Router       Age         Seq#                  Link ID    Interface
10.2.2.2         2007        0x80000005            1          PO0/2/0/0
```

The following is sample outpet from the **show ipv6 ospf database** command with the **grace** keyword:

```
Router# show ipv6 ospf database grace

OSPFv3 Router with ID (10.3.33.3) (Process ID 1)
Grace (Type-11) Link States (Area 0)
  LS age: 2
  LS Type: Grace Links (Interface: Ethernet0/0)
  Link State ID: 3 (Interface ID)
  Advertising Router: 10.2.2.2
  LS Seq Number: 80000001
  Checksum: 0xE3DD
  Length: 36
  Grace Period : 120
        Graceful Restart Reason : Software reload/upgrade
```

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

Table 25: show ipv6 ospf database Field Descriptions

Field	Description
Grace (Type-11)	Type 11 indicates that this router is graceful-restart capable.
LS Type: Grace Links (Interfece: Ethernet 0/0)	The link state type and interface used.
Grace Period : 120	The graceful-restart interval, in seconds.
Graceful Restart Reason: Software reload/upgrade	The reason graceful restart was activated .

Related Commands

Command	Description
show ipv6 ospf	Displays general information about OSPFv3 routing processes.
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.
show ipv6 ospf interface	Displays OSPFv3-related interface information.

show ipv6 ospf event

To display detailed information about IPv6 Open Shortest Path First (OSPF) events, use the **show ipv6 ospf event**command in privileged EXEC mode.

show ipv6 ospf [*process-id*] **event** [{**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**}]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
generic	(Optional) Generic information regarding OSPF for IPv6 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
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

An OSPF event log is kept for every OSPF instance. If you enter no keywords with the **show ipv6 ospf event** command, all information in the OSPF event log is displayed. Use the keywords to filter specific information.

Examples

The following example shows scheduling and SPF run events, LSA arrival and LSA generation events, in order from the oldest events to the latest generated events:

```
Router# show ipv6 ospf event spf lsa reverse

OSPFv3 Router with ID (10.0.0.1) (Process ID 1)
1 *Sep 29 11:59:18.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
```

```
Seq# 80007699, Age 3600
3 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
4 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 2
5 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
6 *Sep 29 11:59:18.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 3600
8 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
9 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1, Seq#
80007699, Age 2
10 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
11 *Sep 29 11:59:18.867: Starting SPF
12 *Sep 29 11:59:18.867: Starting Intra-Area SPF in Area 0
16 *Sep 29 11:59:18.867: Starting Inter-Area SPF in area 0
17 *Sep 29 11:59:18.867: Starting External processing
18 *Sep 29 11:59:18.867: Starting External processing in area 0
19 *Sep 29 11:59:18.867: Starting External processing in area 1
20 *Sep 29 11:59:18.867: End of SPF
21 *Sep 29 11:59:19.367: Generate Changed Type-0x2003 LSA, LSID 10.0.0.4, Seq# 80000002,
Age 3600, Area 1, Prefix 3000:11:22::/64
23 *Sep 29 11:59:20.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
24 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
25 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
26 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
27 *Sep 29 11:59:20.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
28 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
29 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1, Seq#
 8000769A, Age 2
30 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
31 *Sep 29 11:59:20.867: Starting SPF
32 *Sep 29 11:59:20.867: Starting Intra-Area SPF in Area 0
36 *Sep 29 11:59:20.867: Starting Inter-Area SPF in area 0
37 *Sep 29 11:59:20.867: Starting External processing
38 *Sep 29 11:59:20.867: Starting External processing in area 0
39 *Sep 29 11:59:20.867: Starting External processing in area 1
40 *Sep 29 11:59:20.867: End of SPF
```

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

Table 26: show ip ospf Field Descriptions

Field	Description
OSPFv3 Router with ID (10.0.0.1) (Process ID 1)	Process ID and OSPF router ID.
Rcv Changed Type-0x2009 LSA	Description of newly arrived LSA.
LSID	Link-state ID of the LSA.
Adv-Rtr	ID of the advertising router.
Seq#	Link state sequence number (detects old or duplicate link state advertisements).
Age	Link state age (in seconds).
Schedule SPF	Enables SPF to run.

Field	Description
Area	OSPF area ID.
Change in LSID	Changed link-state ID of the LSA.
LSA type	LSA type.

show ipv6 ospf flood-list

To display a list of Open Shortest Path First (OSPF) link-state advertisements (LSAs) waiting to be flooded over an interface, use the **s how ipv6 ospf flood-list**command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **flood-list** *interface-type interface-number*

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
interface-type	Interface type over which the LSAs will be flooded.
interface-number	Interface number over which the LSAs will be flooded.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines   Use this command to display OSPF packet pacing.

Examples   The following is sample output from the **show ipv6 ospf flood-list** command:

```
Router# show ipv6 ospf flood-list
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec
 Type    LS ID          ADV RTR         Seq NO      Age    Checksum
 0x2001  0              172.16.6.6      0x80000031  0      0x1971
 Interface FastEthernet0/0, Queue length 0
 Interface ATM3/0, Queue length 0
```

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

Table 27: show ipv6 ospf flood-list Field Descriptions

Field	Description
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)	Identification of the router for which information is displayed.
Interface POS4/0	Interface for which information is displayed.
Queue length	Number of LSAs waiting to be flooded.
Link state retransmission due in	Length of time before next link-state transmission.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ipv6 ospf graceful-restart

To display Open Shortest Path First for IPv6 (OSPFv3) graceful restart information, use the **show ipv6 ospf graceful-restart** command in privileged EXEC mode.

show ipv6 ospf graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **show ipv6 ospf graceful-restart** command to discover information about the OSPFv3 graceful restart feature.

Examples

The following example displays OSPFv3 graceful restart information:

```
Router# show ipv6 ospf graceful-restart
Routing Process "ospf 1"
 Graceful Restart enabled
    restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
 Graceful Restart helper support enabled
 Router status : Active
 Router is running in SSO mode
 OSPF restart state : NO_RESTART
 Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

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

Table 28: show ipv6 ospf graceful-restart Field Descriptions

Field	Description
Routing Process "ospf 1"	The OSPFv3 routing process ID.
Graceful Restart enabled	The graceful restart feature is enabled on this router.
restart-interval limit: 120 sec	The restart-interval limit.

Field	Description
last restart 00:00:15 ago (took 36 secs)	How long ago the last graceful restart occurred, and how long it took to occur.
Graceful Restart helper support enabled	Graceful restart helper mode is enabled. Because graceful restart mode is also enabled on this router, you can identify this router as being graceful-restart capable. A router that is graceful-restart-aware cannot be configured in graceful-restart mode.
Router status : Active	This router is in active, as opposed to standby, mode.
Router is running in SSO mode	The router is in stateful switchover mode.
OSPF restart state : NO_RESTART	The current OSPFv3 restart state.
Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0	The IPv6 addresses of the current router and the checkpoint router.

Related Commands

Command	Description
show ipv6 ospf interface	Displays OSPFv3-related interface information.

show ipv6 ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the **showipv6ospfinterface** command in user EXEC or privileged mode.

show **ipv6** **ospf** [*process-id*] [*area-id*] **interface** [*type* *number*] [**brief**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information about a specified area only.
type number	(Optional) Interface type and number.
brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

Command Modes   User EXEC Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	Command output is changed when authentication is enabled.
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.
12.4(9)T	Command output is changed when encryption is enabled.
12.2(33)SRB	The **brief** keyword was added.
12.4(15)XF	Output displays were modified so that VMI PPPoE interface-based local state values are displayed in the command output when a VMI interface is specified.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	Command output was updated to display graceful restart information.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

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

Examples

show ipv6 ospf interface Standard Output Example

The following is sample output from the **showipv6ospfinterface** command:

```
Router# show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 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
  Index 1/2/2, flood queue length 0
  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 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  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)
```

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

Table 29: show ipv6 ospf interface Field Descriptions

Field	Description
ATM3/0	Status of the physical link and operational status of protocol.
Link Local Address	Interface IPv6 address.
Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3	The area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type POINT_TO_POINT, Cost: 1	Network type and link-state cost.

Field	Description
Transmit Delay	Transmit delay, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until the next hello packet is sent out this interface.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

Cisco IOS Release 12.2(33)SRB Example

The following is sample output of the **showipv6ospfinterface** command when the **brief** keyword is entered.

```
Router# show ipv6 ospf interface brief

Interface    PID   Area          Intf ID    Cost  State Nbrs F/C
VL0          6     0             21         65535 DOWN  0/0
Se3/0        6     0             14         64    P2P   0/0
Lo1          6     0             20         1     LOOP  0/0
Se2/0        6     6             10         62    P2P   0/0
Tu0          1000  0             19         11111 DOWN  0/0
```

OSPF with Authentication on the Interface Example

The following is sample output from the **showipv6ospfinterface** command with authentication enabled on the interface:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication SPI 500, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Null Authentication Example

The following is sample output from the **showipv6ospfinterface** command with null authentication configured on the interface:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  Authentication NULL
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Authentication for the Area Example

The following is sample output from the **showipv6ospfinterface** command with authentication configured for the area:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Dynamic Cost Example

The following display shows sample output from the **showipv6ospfinterface** command when the OSPF cost dynamic is configured.

```
Router1# show ipv6 ospf interface serial 2/0
```

```
Serial2/0 is up, line protocol is up
   Link Local Address 2001:0DB1:A8BB:CCFF:FE00:100, Interface ID 10
   Area 1, Process ID 1, Instance ID 0, Router ID 172.1.1.1
   Network Type POINT_TO_MULTIPOINT, Cost: 64 (dynamic), Cost Hysteresis: 200
   Cost Weights: Throughput 100, Resources 20, Latency 80, L2-factor 100
   Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
   Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
     Hello due in 00:00:19
   Index 1/2/3, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
```

OSPF Graceful Restart Example

The following display shows sample output from the **showipv6ospfinterface** command when the OSPF graceful restart feature is configured:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:300, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.3.3.3
  Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Graceful Restart p2p timeout in 00:00:19
     Hello due in 00:00:02
  Graceful Restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.1.1
  Suppress hello for 0 neighbor(s)
```

Example of an Enabled Protocol

The following display shows that the OSPF interface is enabled for Bidirectional Forwarding Detection (BFD):

```
Router# show ipv6 ospf interface
Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

Related Commands

Command	Description
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.

show ipv6 ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on a per-interface basis, use the **show ipv6 ospf neighbor** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
interface-type interface-number	(Optional) Interface type and number.
neighbor-id	(Optional) Neighbor ID.
detail	(Optional) Displays all neighbors in detail (lists all neighbors).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	Command output for the **detail** keyword was updated to display graceful-restart information.
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 ipv6 ospf neighbor** command:

```
Router# show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID   Interface
172.16.4.4       1    FULL/  -        00:00:31    14             POS4/0
172.16.3.3       1    FULL/BDR        00:00:30    3              FastEthernet00
172.16.5.5       1    FULL/  -        00:00:33    13             ATM3/0
```

The following is sample output from the **show ipv6 ospf neighbor** command with the **detail** keyword:

```
Router# show ipv6 ospf neighbor detail
 Neighbor 172.16.4.4
    In the area 0 via interface POS4/0
    Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63AD1B0D
    Dead timer due in 00:00:33
    Neighbor is up for 00:48:56
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.3.3
    In the area 1 via interface FastEthernet0/0
    Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 172.16.6.6 BDR is 172.16.3.3
    Options is 0x63F813E9
    Dead timer due in 00:00:33
    Neighbor is up for 00:09:00
    Index 1/1/2, retransmission queue length 0, number of retransmission 2
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.5.5
    In the area 2 via interface ATM3/0
    Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63F7D249
    Dead timer due in 00:00:38
    Neighbor is up for 00:10:01
    Index 1/1/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

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

Table 30: show ipv6 ospf neighbor Field Descriptions

Field	Description
Neighbor ID; Neighbor	Neighbor router ID.
In the area	Area and interface through which the OSPF neighbor is known.
Pri; Neighbor priority	Router priority of the neighbor, neighbor state.
State	OSPF state.
State changes	Number of state changes since the neighbor was created.
Options	Hello packet options field contents. (E-bit only. Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)
Dead timer due in	Expected time before Cisco IOS software will declare the neighbor dead.

Field	Description
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into two-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in the retransmission queue.
number of retransmission	Number of times update packets have been re-sent during flooding.
First	Memory location of the flooding details.
Next	Memory location of the flooding details.
Last retransmission scan length	Number of link state advertisements (LSAs) in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build last retransmission packet.
maximum	Maximum time taken to build any retransmission packet.

The following is sample output from the **show ipv6 ospf neighbor** command with the **detail** keyword, displaying graceful-restart information:

```
Router# show ipv6 ospf neighbor detail
 Neighbor 10.1.1.1
    In the area 0 via interface Ethernet0/0
    Neighbor: interface-id 3, link-local address FE80::A8BB:CCFF:FE00:200
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.1.1.1 BDR is 10.3.3.3
    Options is 0x1C9AD11
    Neighbor graceful restart timer due in 00:01:44
    Last neighbor graceful restart 01:00:19 ago
    Dead timer due in 00:00:36
    Neighbor is up for 00:00:16
    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
```

show ipv6 ospf request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **s how ipv6 ospf request-list**command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the Open Shortest Path First (OSPF) routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
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
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The information displayed by the **show ipv6 ospf request-list** command is useful in debugging OSPF routing operations.

Examples

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

```
Router# show ipv6 ospf 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 31: show ipv6 ospf 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 ipv6 ospf retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the **s how ipv6 ospf retransmission-list**command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
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
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The information displayed by the **show ipv6 ospf retransmission-list** command is useful in debugging Open Shortest Path First (OSPF) routing operations.

Examples

The following is sample output from the **show ipv6 ospf retransmission-list** command:

```
Router# show ipv6 ospf 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 32: show ipv6 ospf 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 ipv6 ospf statistics

To display Open Shortest Path First for IPv6 (OSPFv6) shortest path first (SPF) calculation statistics, use the **show ipv6 ospf statistics** command in user EXEC or privileged EXEC mode.

show ipv6 ospf statistics [**detail**]

Syntax Description

detail	(Optional) Displays statistics separately for each OSPF area and includes additional, more detailed statistics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	**Modification**
12.2(33)SRC	This command was introduced.

Usage Guidelines

The **show ipv6 ospf 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 ipv6 ospf statistics** command is recommended as the first troubleshooting step for link-state advertisement (LSA) flapping.

Examples

The following example provides detailed statistics for each OSPFv6 area:

```
Router# show ipv6 ospf 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
  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 33: show ipv6 ospf 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.
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 ipv6 ospf summary-prefix

To display a list of all summary address redistribution information configured under an OSPF process, use the **s how ipv6 ospf summary-prefix**command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] **summary-prefix**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The *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 ipv6 ospf summary-prefix** command:

```
Router# show ipv6 ospf 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 34: show ipv6 ospf 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 ipv6 ospf timers rate-limit

To display all of the link-state advertisements (LSAs) in the rate limit queue, use the **show ipv6 ospf timers rate-limit** command in privileged EXEC mode.

show ipv6 ospf timers rate-limit

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **show ipv6 ospf timers rate-limit** command to discover when LSAs in the queue will be sent.

Examples

show ipv6 ospf timers rate-limit Output Example

The following is sample output from the **show ipv6 ospf timers rate-limit** command:

```
Router# show ipv6 ospf 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 35: show ipv6 ospf 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 ipv6 ospf traffic

To display IPv6 Open Shortest Path First Version 3 (OSPFv3) traffic statistics, use the **showipv6ospftraffic**command in privileged EXEC mode.

show ipv6 ospf [*process-id*] **traffic** [*interface-type interface-number*]

Syntax Description

process-id	(Optional) OSPF process ID for which you want traffic statistics (for example, queue statistics, statistics for each interface under the OSPF process, and per OSPF process statistics).
interface-type interface-number	(Optional) Type and number associated with a specific OSPF interface.

Command Default

When the **showipv6ospftraffic** command is entered without any arguments, global OSPF traffic statistics are displayed, including queue statistics for each OSPF process, statistics for each interface, and per OSPF process statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

You can limit the displayed traffic statistics to those for a specific OSPF 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 OSPF process by entering values for the *interface-type* and *interface-number* arguments. To reset counters and clear statistics, use the **clearipv6ospftraffic** command.

Examples

The following example shows the display output for the **showipv6ospftraffic** command for OSPFv3:

```
Router# show ipv6 ospf 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 network administrator wants to start collecting new statistics, resetting the counters and clearing the traffic statistics by entering the **clearipv6ospftraffic** command as follows:

```
Router# clear ipv6 ospf traffic
```

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

Table 36: show ipv6 ospf traffic Field Descriptions

Field	Description
OSPFv3 statistics	Traffic statistics accumulated for all OSPF processes running on the router. To ensure compatibility with the **showiptraffic** 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 OSPF hello process for all received OSPF packets.
Router queue	Statistics for the internal Cisco IOS queue between the OSPF hello process and the OSPF router for all received OSPF packets except OSPF 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.
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 OSPF link-state advertisement (LSA). The discarded packet is counted under the appropriate discard reason.

Field	Description
Summary traffic statistics for process ID	Summary traffic statistics accumulated for an OSPFv3 process.
	Note The OSPF 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 OSPF statistics.

Related Commands

Command	Description
clear ip ospf traffic	Clears OSPFv2 traffic statistics.
clear ipv6 ospf traffic	Clears OSPFv3 traffic statistics.
show ip ospf traffic	Displays OSPFv2 traffic statistics.

show ipv6 ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **s how ipv6 ospf virtual-links** command in user EXEC or privileged EXEC mode.

show ipv6 ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	Command output was updated to display OSPF for IPv6 encryption information.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The information displayed by the **show ipv6 ospf virtual-links** command is useful in debugging OSPF routing operations.

Examples

The following is sample output from the **show ipv6 ospf virtual-links** command:

```
Router# show ipv6 ospf 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 37: show ipv6 ospf virtual-links Field Descriptions

Field	Description
Virtual Link OSPF_VL0 to router 172.16.6.6 is up	Specifies the OSPF neighbor, and if the link to that neighbor is up or down.

Field	Description
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 OSPF 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 OSPF 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 ipv6 ospf virtual-links** command has two virtual links. One is protected by authentication, and the other is protected by encryption.

```
Router# show ipv6 ospf 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 ipv6 pim anycast-RP

To verify IPv6 PIM anycast RP operation, use the **show ipv6 pim anycast-RP** command in user EXEC or privileged EXEC mode.

show ipv6 pim anycast-RP *rp-address*

Syntax Description

rp-address	RP address to be verified.

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

Usage Guidelines

Examples

```
Router# show ipv6 pim anycast-rp 110::1:1:1

Anycast RP Peers For 110::1:1:1   Last Register/Register-Stop received
  20::1:1:1 00:00:00/00:00:00
```

Related Commands

Command	Description
ipv6 pim anycast-RP	Configures the address of the PIM RP for an anycast group range.

show ipv6 pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ipv6 pim bsr** command in user EXEC or privileged EXEC mode.

show **ipv6** **pim** [**vrf** *vrf-name*] **bsr** {**election** | **rp-cache** | **candidate-rp**}

Syntax Description

vrf	*vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
election		Displays BSR state, BSR election, and bootstrap message (BSM)-related timers.
rp-cache		Displays candidate rendezvous point (C-RP) cache learned from unicast C-RP announcements on the elected BSR.
candidate-rp		Displays C-RP state on devices that are configured as C-RPs.

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.
12.0(28)S	The **election**, **rp-cache**, and **candidate-rp** keywords were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **election**, **rp-cache**, and **candidate-rp** 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 introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.7S	Command output when using the **election** keyword was modified.

Usage Guidelines

Use the **show ipv6 pim bsr** command to display details of the BSR election-state machine, C-RP advertisement state machine, and the C-RP cache. Information on the C-RP cache is displayed only on the elected BSR device, and information on the C-RP state machine is displayed only on a device configured as a C-RP.

Examples

The following example displays BSM election information:

```
device# show ipv6 pim bsr election
PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126
```

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

Table 38: show ipv6 pim bsr election Field Descriptions

Field	Description
Scope Range List	Scope to which this BSR information applies.
This system is the Bootstrap Router (BSR)	Indicates this device is the BSR and provides information on the parameters associated with it.
BS Timer	On the elected BSR, the BS timer shows the time in which the next BSM will be originated. On all other devices in the domain, the BS timer shows the time at which the elected BSR expires.
This system is candidate BSR	Indicates this device is the candidate BSR and provides information on the parameters associated with it.

The following example displays information that has been learned from various C-RPs at the BSR. In this example, two candidate RPs have sent advertisements for the FF00::/8 or the default IPv6 multicast range:

```
Device# show ipv6 pim bsr rp-cache
PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) FF00::/8, RP count 2
  RP 10::1:1:3
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:55
  RP 20::1:1:1
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:5
```

The following example displays information about the C-RP. This RP has been configured without a specific scope value, so the RP will send C-RP advertisements to all BSRs about which it has learned through BSMs it has received.

```
Device# show ipv6 pim bsr candidate-rp
PIMv2 C-RP information
    Candidate RP: 10::1:1:3
      All Learnt Scoped Zones, Priority 192, Holdtime 150
      Advertisement interval 60 seconds
      Next advertisement in 00:00:33
```

The following example confirms that the IPv6 C-BSR is PIM-enabled. If PIM is disabled on an IPv6 C-BSR interface, or if a C-BSR or C-RP is configured with the address of an interface that does not have PIM enabled, the **show ipv6 pim bsr** command used with the **election** keyword would display that information instead.

```
Device# show ipv6 pim bsr election

PIMv2 BSR information

BSR Election Information
  Scope Range List: ff00::/8
     BSR Address: 2001:DB8:1:1:2
     Uptime: 00:02:42, BSR Priority: 34, Hash mask length: 28
     RPF: FE80::20:1:2,Ethernet1/0
     BS Timer: 00:01:27
```

show ipv6 pim df

To display the designated forwarder (DF)-election state of each interface for each rendezvous point (RP), use the **show ipv6 pim df**command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*]

Syntax Description		
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
rp-address	(Optional) RP IPv6 address.

Command Default

If no interface or RP address is specified, all DFs are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)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	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 pim df** command to display the state of the DF election for each RP on each Protocol Independent Multicast (PIM)-enabled interface if the bidirectional multicast traffic is not flowing as expected.

Examples

The following example displays the DF-election states:

```
Router# show ipv6 pim df
Interface       DF State    Timer       Metrics
Ethernet0/0     Winner      4s 8ms      [120/2]
    RP :200::1
Ethernet1/0     Lose        0s 0ms      [inf/inf]
    RP :200::1
```

The following example shows information on the RP:

```
Router# show ipv6 pim df
Interface          DF State    Timer        Metrics
Ethernet0/0        None:RP LAN 0s 0ms        [inf/inf]
    RP :200::1
Ethernet1/0        Winner      7s 600ms      [0/0]
    RP :200::1
Ethernet2/0        Winner      9s 8ms        [0/0]
    RP :200::1
```

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

Table 39: show ipv6 pim df Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
DF State	The state of the DF election on the interface. The state can be: • Offer • Winner • Backoff • Lose • None:RP LAN The None:RP LAN state indicates that no DF election is taking place on this LAN because the RP is directly connected to this LAN.
Timer	DF election timer.
Metrics	Routing metrics to the RP announced by the DF.
RP	The IPv6 address of the RP.

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

show ipv6 pim df winner

To display the designated forwarder (DF)-election winner on each interface for each rendezvous point (RP), use the **show ipv6 pim df winner**command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **df winner** [*interface-type interface-number*] [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
rp-address	(Optional) RP IPv6 address.

Command Default

If no interface or RP address is specified, all DFs are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	**Modification**
12.3(7)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	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 pim df winner** command to display the DF election winner for each RP on each Protocol Independent Multicast (PIM)-enabled interface if the bidirectional multicast traffic is not flowing as expected.

Examples

The following example shows the DF winner for the IPv6 address 200::1:

```
Router# show ipv6 pim df winner ethernet 1/0 200::1
Interface        Metrics
Ethernet1/0      [120/2]
RP         : 200::1
DF Winner : FE80::A8BB:CCFF:FE00:601
```

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

Table 40: show ipv6 pim df winner Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
Metrics	Routing metrics to the RP announced by the DF.
RP	The IPv6 address of the RP.
DF Winner	The IPv6 address of the DF election winner.

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
show ipv6 pim df	Displays the DF -election state of each interface for each RP.

show ipv6 pim group-map

To display an IPv6 Protocol Independent Multicast (PIM) group mapping table, use the **show ipv6 pim group-map** command in user EXEC or privileged EXEC mode.

{**show ipv6 pim** [**vrf** *vrf-name*] **group-map** [{*group-namegroup-address*}] | [{*group-rangegroup-mask*}] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
group-range | *group-mask*	(Optional) Group range list. Includes group ranges with the same prefix or mask length.
info-source	(Optional) Displays all mappings learned from a specific source, such as the bootstrap router (BSR) or static configuration.
bsr	Displays ranges learned through the BSR.
default	Displays ranges enabled by default.
embedded-rp	Displays group ranges learned through the embedded rendezvous point (RP).
static	Displays ranges enabled by static configuration.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.0(28)S	The *group-range* and *group-mask* arguments were added, and the **info-source bsr**, **static**, and **default** keywords were added.
12.2(25)S	The *group-range* and *group-mask* arguments were added, and the **info-source bsr**, **static**, and **default** keywords were added.
12.3(11)T	The *group-range* and *group-mask* arguments were added, and the **info-source bsr**, **static**, and **default** 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.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **show ipv6 pim group-map** command to find all group mappings installed by a given source of information, such as BSR or static configuration.

You can also use this command to find which group mapping a router at a specified IPv6 group address is using by specifying a group address, or to find an exact group mapping entry by specifying a group range and mask length.

Examples

The following is sample output from the **show ipv6 pim group-map**command:

```
Router# show ipv6 pim group-map
FF33::/32*
     SSM
     Info source:Static
     Uptime:00:08:32, Groups:0
 FF34::/32*
     SSM
     Info source:Static
     Uptime:00:09:42, Groups:0
```

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

Table 41: show ipv6 pim group-map Field Descriptions

Field	Description
RP	Address of the RP router if the protocol is sparse mode or bidir.
Protocol	Protocol used: sparse mode (SM), Source Specific Multicast (SSM), link-local (LL), or NOROUTE (NO).
	LL is used for the link-local scoped IPv6 address range (ff[0-f]2::/16). LL is treated as a separate protocol type, because packets received with these destination addresses are not forwarded, but the router might need to receive and process them.
	NOROUTE or NO is used for the reserved and node-local scoped IPv6 address range (ff[0-f][0-1]::/16). These addresses are nonroutable, and the router does not need to process them.
Groups	How many groups are present in the topology table from this range.
Info source	Mappings learned from a specific source; in this case, static configuration.
Uptime	The uptime for the group mapping displayed.

The following example displays the group mappings learned from BSRs that exist in the PIM group-to-RP or mode-mapping cache. The example shows the address of the BSR from which the group mappings have been learned and the associated timeout.

```
Router# show ipv6 pim group-map info-source bsr
FF00::/8*
    SM, RP: 20::1:1:1
    RPF: Et1/0,FE80::A8BB:CCFF:FE03:C202
    Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
    Uptime: 00:19:51, Groups: 0
FF00::/8*
    SM, RP: 10::1:1:3
    RPF: Et0/0,FE80::A8BB:CCFF:FE03:C102
    Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
    Uptime: 00:19:51, Groups: 0
```

show ipv6 pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ipv6 pim interface** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
state-on	(Optional) Displays interfaces with PIM enabled.
state-off	(Optional) Displays interfaces with PIM disabled.
type number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **state-on** and **state-off**keywords were added.
12.3(4)T	The **state-on** and **state-off**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 2.6	Command output was modified to display passive interface information.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

The **show ipv6 pim interface** command is used to check if PIM is enabled on an interface, the number of neighbors, and the designated router (DR) on the interface.

Examples

The following is sample output from the **show ipv6 pim interface** command using the **state-on** keyword:

```
Router# show ipv6 pim interface state-on
Interface          PIM  Nbr   Hello  DR
                        Count Intvl  Prior
```

```
Ethernet0          on   0    30    1
    Address:FE80::208:20FF:FE08:D7FF
    DR    :this system
POS1/0             on   0    30    1
    Address:FE80::208:20FF:FE08:D554
    DR    :this system
POS4/0             on   1    30    1
    Address:FE80::208:20FF:FE08:D554
    DR    :FE80::250:E2FF:FE8B:4C80
POS4/1             on   0    30    1
    Address:FE80::208:20FF:FE08:D554
    DR    :this system
Loopback0          on   0    30    1
    Address:FE80::208:20FF:FE08:D554
    DR    :this system
```

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

Table 42: show ipv6 pim interface Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
PIM	Whether PIM is enabled on an interface.
Nbr Count	Number of PIM neighbors that have been discovered through this interface.
Hello Intvl	Frequency, in seconds, of PIM hello messages.
DR	IP address of the designated router (DR) on a network.
Address	Interface IP address of the next-hop router.

The following is sample output from the **show ipv6 pim interface** command, modified to display passive interface information:

```
Router(config)# show ipv6 pim interface gigabitethernet0/0/0

    Interface            PIM   Nbr   Hello  DR  BFD
                               Count Intvl Prior

    GigabitEthernet0/0/0  on/P  0     30     1   On
        Address: FE80::A8BB:CCFF:FE00:9100
        DR    : this system
```

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

Table 43: show ipv6 pim interface Field Description

Field	Description
PIM	Whether PIM is enabled on an interface. When PIM passive mode is used, a "P" is displayed in the output.

Related Commands	Command	Description
	show ipv6 pim neighbor	Displays the PIM neighbors discovered by the Cisco IOS software.

show ipv6 pim join-prune statistic

To display the average join-prune aggregation for the most recently aggregated 1000, 10,000, and 50,000 packets for each interface, use the **show ipv6 pim join-prune statistic** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.

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(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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

When Protocol Independent Multicast (PIM) sends multiple joins and prunes simultaneously, it aggregates them into a single packet. The **show ipv6 pim join-prune statistic** command displays the average number of joins and prunes that were aggregated into a single packet over the last 1000 PIM join-prune packets, over the last 10,000 PIM join-prune packets, and over the last 50,000 PIM join-prune packets.

Examples

The following example provides the join/prune aggregation on Ethernet interface 0/0/0:

```
Router# show ipv6 pim join-prune statistic Ethernet0/0/0
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface           Transmitted           Received
Ethernet0/0/0     0   / 0   / 0        1   / 0   / 0
```

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

Table 44: show ipv6 pim join-prune statistics Field Descriptions

Field	Description
Interface	The interface from which the specified packets were transmitted or on which they were received.
Transmitted	The number of packets transmitted on the interface.
Received	The number of packets received on the interface.

show ipv6 pim limit

To display Protocol Independent Multicast (PIM) interface limit, use the **show ipv6 pim limit** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **limit** [*interface*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface	(Optional) Specific interface for which limit information is provided.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 pim limit** command checks interface statistics for limits. If the optional *interface* argument is enabled, only information for the specified interface is shown.

Examples

The following example displays s PIM interface limit information:

```
Router# show ipv6 pim limit
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.
ipv6 multicast limit cost	Applies a cost to mroutes that match per interface mroute state limiters in IPv6.

show ipv6 pim neighbor

To display the Protocol Independent Multicast (PIM) neighbors discovered by the Cisco software, use the **show ipv6 pim neighbor** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **neighbor** [**detail**] [*interface-type interface-number* | **count**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
detail	(Optional) Displays the additional addresses of the neighbors learned, if any, through the routable address hello option.
interface-type interface-number	(Optional) Interface type and number.
count	(Optional) Displays neighbor counts on each interface.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf***vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines   The **show ipv6 pim neighbor** command displays which routers on the LAN are configured for PIM.

Examples   The following is sample output from the **show ipv6 pim neighbor** command using the detail keyword to identify the additional addresses of the neighbors learned through the routable address hello option:

```
Router# show ipv6 pim neighbor detail

Neighbor Address(es)     Interface        Uptime    Expires DR pri Bidir

FE80::A8BB:CCFF:FE00:401  Ethernet0/0      01:34:16  00:01:16 1      B
60::1:1:3
```

```
FE80::A8BB:CCFF:FE00:501   Ethernet0/0        01:34:15  00:01:18 1     B
60::1:1:4
```

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

Table 45: show ipv6 pim neighbor Field Descriptions

Field	Description
Neighbor addresses	IPv6 address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	How long (in hours, minutes, and seconds) the entry has been in the PIM neighbor table.
Expires	How long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table.
DR	Indicates that this neighbor is a designated router (DR) on the LAN.
pri	DR priority used by this neighbor.
Bidir	The neighbor is capable of PIM in bidirectional mode.

Related Commands

Command	Description
show ipv6 pim interfaces	Displays information about interfaces configured for PIM.

show ipv6 pim range-list

To display information about IPv6 multicast range lists, use the **show ipv6 pim range-list**command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **range-list** [**config**] [{*rp-addressrp-name*}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
config	(Optional) The client. Displays the range lists configured on the router.
*rp-address	rp-name*	(Optional) The address of a Protocol Independent Multicast (PIM) rendezvous point (RP).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **show ipv6 pim range-list** command displays IPv6 multicast range lists on a per-client and per-mode basis. A client is the entity from which the specified range list was learned. The clients can be config, and the modes can be Source Specific Multicast (SSM) or sparse mode (SM).

Examples

The following is sample output from the **show ipv6 pim range-list**command:

```
Router# show ipv6 pim range-list
config SSM Exp:never Learnt from :::
 FF33::/32 Up:00:26:33
 FF34::/32 Up:00:26:33
 FF35::/32 Up:00:26:33
 FF36::/32 Up:00:26:33
```

```
FF37::/32 Up:00:26:33
FF38::/32 Up:00:26:33
FF39::/32 Up:00:26:33
FF3A::/32 Up:00:26:33
FF3B::/32 Up:00:26:33
FF3C::/32 Up:00:26:33
FF3D::/32 Up:00:26:33
FF3E::/32 Up:00:26:33
FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
 FF13::/64 Up:00:03:50
config SM RP:40::1:1:3 Exp:never Learnt from :::
 FF09::/64 Up:00:03:50
```

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

Table 46: show ipv6 pim range-list Field Descriptions

Field	Description
config	Config is the client.
SSM	Protocol being used.
FF33::/32	Group range.
Up:	Uptime.

show ipv6 pim topology

To display Protocol Independent Multicast (PIM) topology table information for a specific group or all groups, use the **show ipv6 pim topology** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **topology** [{*groupname-or-address* [*sourcename-or-address*] | **link-local** | **route-count** [**detail**]}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
groupname-or-address	(Optional) IPv6 address or name of the multicast group.
sourcename-or-address	(Optional) IPv6 address or name of the source.
link-local	(Optional) Displays the link-local groups.
route-count	(Optional) Displays the number of routes in PIM topology table.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was modified. The **link-local** keyword was added.
12.3(4)T	This command was modified. The **link-local** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

This command shows the PIM topology table for a given group--(*, G), (S, G), and (S, G) Rendezvous Point Tree (RPT)-- as internally stored in a PIM topology table. The PIM topology table may have various entries for a given group, each with its own interface list. The resulting forwarding state is maintained in the Multicast

Routing Information Base (MRIB) table, which shows which interface the data packet should be accepted on and which interfaces the data packet should be forwarded to for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

The **route-count** keyword shows the count of all entries, including link-local entries.

PIM communicates the contents of these entries through the MRIB, which is an intermediary for communication between multicast routing protocols (such as PIM), local membership protocols (such as Multicast Listener Discovery [MLD]), and the multicast forwarding engine of the system.

For example, an interface is added to the (*, G) entry in PIM topology table upon receipt of an MLD report or PIM (*, G) join message. Similarly, an interface is added to the (S, G) entry upon receipt of the MLD INCLUDE report for the S and G or PIM (S, G) join message. Then PIM installs an (S, G) entry in the MRIB with the immediate olist (from (S, G)) and the inherited olist (from (*, G)). Therefore, the proper forwarding state for a given entry (S, G) can be seen only in the MRIB or the MFIB, not in the PIM topology table.

Examples

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

```
Router# show ipv6 pim topology
IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary
(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:40::1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1          02:26:56  fwd LI LH
(50::1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1          00:00:07  off LI
```

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

Table 47: show ipv6 pim topology Field Descriptions

Field	Description
Entry flags: KAT	The keepalive timer (KAT) associated with a source is used to keep track of two intervals while the source is alive. When a source first becomes active, the first-hop router sets the keepalive timer to 3 minutes and 30 seconds, during which time it does not probe to see if the source is alive. Once this timer expires, the router enters the probe interval and resets the timer to 65 seconds, during which time the router assumes the source is alive and starts probing to determine if it actually is. If the router determines that the source is alive, the router exits the probe interval and resets the keepalive timer to 3 minutes and 30 seconds. If the source is not alive, the entry is deleted at the end of the probe interval.
AA, PA	The assume alive (AA) and probe alive (PA) flags are set when the router is in the probe interval for a particular source.

Field	Description
RR	The register received (RR) flag is set on the (S, G) entries on the Route Processor (RP) as long as the RP receives registers from the source Designated Router (DR), which keeps the source state alive on the RP.
SR	The sending registers (SR) flag is set on the (S, G) entries on the DR as long as it sends registers to the RP.

Related Commands

Command	Description
show ipv6 mrib client	Displays information about the clients of the MRIB.
show ipv6 mrib route	Displays MRIB route information.

show ipv6 pim traffic

To display the Protocol Independent Multicast (PIM) traffic counters, use the **show ipv6 pim traffic** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

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(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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **show ipv6 pim traffic** command to check if the expected number of PIM protocol messages have been received and sent.

Examples

The following example shows the number of PIM protocol messages received and sent.

```
Router# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29
                              Received      Sent
Valid PIM Packets                22          22
Hello                            22          22
Join-Prune                        0           0
Register                          0           0
Register Stop                     0           0
Assert                            0           0
Bidir DF Election                 0           0
Errors:
Malformed Packets                             0
Bad Checksums                                 0
Send Errors                                   0
Packet Sent on Loopback Errors                0
```

```
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
```

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

Table 48: show ipv6 pim traffic Field Descriptions

Field	Description
Elapsed time since counters cleared	Indicates the amount of time (in hours, minutes, and seconds) since the counters cleared.
Valid PIM Packets	Number of valid PIM packets received and sent.
Hello	Number of valid hello messages received and sent.
Join-Prune	Number of join and prune announcements received and sent.
Register	Number of PIM register messages received and sent.
Register Stop	Number of PIM register stop messages received and sent.
Assert	Number of asserts received and sent.

show ipv6 pim tunnel

To display information about the Protocol Independent Multicast (PIM) register encapsulation and de-encapsulation tunnels on an interface, use the **show ipv6 pim tunnel**command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Tunnel interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

If you use the **show ipv6 pim tunnel** command without the optional *interface* keyword, information about the PIM register encapsulation and de-encapsulation tunnel interfaces is displayed.

The PIM encapsulation tunnel is the register tunnel. An encapsulation tunnel is created for every known rendezvous point (RP) on each router. The PIM decapsulation tunnel is the register decapsulation tunnel. A decapsulation tunnel is created on the RP for the address that is configured to be the RP address.

Examples

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

```
Router# show ipv6 pim tunnel
Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:100::1
Tunnel0*
```

```
Type  :PIM Decap
RP    :100::1
Source: -
```

The following is sample output from the **show ipv6 pim tunnel**command on a non-RP:

```
Router# show ipv6 pim tunnel
Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:2001::1:1:1
```

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

Table 49: show ipv6 pim tunnel Field Descriptions

Field	Description
Tunnel0*	Name of the tunnel.
Type	Type of tunnel. Can be PIM encapsulation or PIM de-encapsulation.
source	Source address of the router that is sending encapsulating registers to the RP.

show ipv6 policy

To display the IPv6 policy-based routing (PBR) configuration, use the **show ipv6 policy** command in user EXEC or privileged EXEC mode.

show ipv6 policy

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

IPv6 policy matches will be counted on route maps, as is done in IPv4. Therefore, IPv6 policy matches can also be displayed on the **show route-map** command.

Examples

The following example displays the PBR configuration:

```
Device# show ipv6 policy

Interface                 Routemap
Ethernet0/0               src-1
```

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

Field	Description
Interface	Interface type and number that is configured to run Protocol-Independent Multicast (PIM).
Routemap	The name of the route map on which IPv6 policy matches were counted.

Related Commands

Command	Description
show route-map	Displays all route maps configured or only the one specified.

show ipv6 port-map

To verify port-to-application mapping (PAM) configuration, use the **show ipv6 port-map**command in user EXEC or privileged EXEC mode.

show ipv6 port-map [{*application* | **port** *port-number*}]

Syntax Description		
application	(Optional) Specifies the name of the application used in port mapping.	
port *port-number*	(Optional) Specifies the port number that maps to the application.	

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **show ipv6 port-map** command displays the entire IPv6 port-mapping table or specific port-mapping information of a particular port number or application (protocol). Enabling the **show ipv6 port-map** command displays the entire IPv6 PAM table, including system-defined, user-defined, and host-specific port-mapping configurations.

To display port-mapping details of a specific port number, use the **show ipv6 port-map** command with the **port***port-number* keyword and argument.

To display the port-mapping details of a specific application, use the **show ipv6 port-map** command with the *application* argument.

Examples

The following example displays the FTP application's PAM information:

```
Router# show ipv6 port-map ftp
```

The following example displays PAM information at port number 21:

```
Router# show ipv6 port-map port 21
```

Related Commands

Command	Description
ipv6 port-map	Establishes PAM for the system.

show ipv6 prefix-list

To display information about an IPv6 prefix list or IPv6 prefix list entries, use the **show ipv6 prefix-list**command in user EXEC or privileged EXEC mode.

show ipv6 prefix-list [{**detail** | **summary**}] [*list-name*]
show ipv6 prefix-list *list-name* *ipv6-prefix/prefix-length* [{**longer** | **first-match**}]
show ipv6 prefix-list *list-name* **seq** *seq-num*

Syntax Description

detail | **summary**	(Optional) Displays detailed or summarized information about all IPv6 prefix lists.
list-name	(Optional) The name of a specific IPv6 prefix list.
ipv6-prefix	All prefix list entries for the specified 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*	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	(Optional) Displays all entries of an IPv6 prefix list that are more specific than the given *ipv6-prefix / prefix-length*values.
first-match	(Optional) Displays the entry of an IPv6 prefix list that matches the given *ipv6-prefix / prefix-length*values.
seq *seq-num*	The sequence number of the IPv6 prefix list entry.

Command Default   Displays information about all IPv6 prefix lists.

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.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

Examples

The following example shows the output of the **show ipv6 prefix-list** command with the **detail** keyword:

```
Router# show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
   seq 5 permit 2002::/16 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
   seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
   seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
   seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
   seq 10 deny ::/0 (hit count: 0, refcount: 1)
   seq 15 deny ::/1 (hit count: 0, refcount: 1)
   seq 20 deny ::/2 (hit count: 0, refcount: 1)
   seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
   seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

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

Table 50: show ipv6 prefix-list Field Descriptions

Field	Description
Prefix list with the latest deletion/insertion:	Prefix list that was last modified.
count	Number of entries in the list.
range entries	Number of entries with matching range.
sequences	Sequence number for the prefix entry.
refcount	Number of objects currently using this prefix list.
seq	Entry number in the list.
permit, deny	Granting status.
hit count	Number of matches for the prefix entry.

The following example shows the output of the **show ipv6 prefix-list** command with the **summary**keyword:

```
Router# show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
```

```
    count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
ipv6 prefix-list aggregate:
    count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
ipv6 prefix-list bgp-in:
    count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

Related Commands

Command	Description
clear ipv6 prefix-list	Resets the hit count of the prefix list entries.
distribute-list in	Filters networks received in updates.
distribute-list out	Suppresses networks from being advertised in updates.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 prefix-list description	Adds a text description of an IPv6 prefix list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
remark (prefix-list)	Adds a comment for an entry in a prefix list.

show ipv6 protocols

To display the parameters and the current state of the active IPv6 routing protocol processes, use the **show ipv6 protocols** command in user EXEC or privileged EXEC mode.

show ipv6 protocols [**summary**]

Syntax Description	**summary** | (Optional) Displays the configured routing protocol process names.

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
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.
12.4(15)T	This command was modified. The command output was enhanced to provide Enhanced Interior Gateway Routing Protocol (EIGRP) information, including the vector metric.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.4	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.6	This command was modified. The command output was enhanced to include information about EIGRP IPv6 Nonstop Forwarding (NSF).
15.2(2)S	This command was modified. The command output was enhanced to include information about EIGRP IPv6 NSF.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines   The information displayed by the **show ipv6 protocols** command is useful in debugging routing operations.

Examples   The following sample output from the **show ipv6 protocols** command displays Intermediate System-to-Intermediate System (IS-IS) routing protocol information:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Inter-area redistribution
    Redistributing L1 into L2 using prefix-list word
  Address Summarization:
    L2: 33::/16  advertised with metric 0
    L2: 44::/16  advertised with metric 20
    L2: 66::/16  advertised with metric 10
    L2: 77::/16  advertised with metric 10
```

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

Table 51: show ipv6 protocols Field Descriptions for IS-IS Processes

Field	Description
IPv6 Routing Protocol is	Specifies the IPv6 routing protocol used.
Interfaces	Specifies the interfaces on which the IPv6 IS-IS protocol is configured.
Redistribution	Lists the protocol that is being redistributed.
Inter-area redistribution	Lists the IS-IS levels that are being redistributed into other levels.
using prefix-list	Names the prefix list used in the interarea redistribution.
Address Summarization	Lists all the summary prefixes. If the summary prefix is being advertised, "advertised with metric x" will be displayed after the prefix.

The following sample output from the **show ipv6 protocols** command displays the Border Gateway Protocol (BGP) information for autonomous system 30:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "bgp 30"
  IGP synchronization is disabled
  Redistribution:
    Redistributing protocol connected
  Neighbor(s):
```

```
Address                  FiltIn FiltOut Weight RoutemapIn RoutemapOut
2001:DB8:0:ABCD::1          5       7     200
2001:DB8:0:ABCD::2                               rmap-in    rmap-out
2001:DB8:0:ABCD::3                               rmap-in    rmap-out
```

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

Table 52: show ipv6 protocols Field Descriptions for BGP Process

Field	Description
IPv6 Routing Protocol is	Specifies the IPv6 routing protocol used.
Redistribution	Lists the protocol that is being redistributed.
Address	Neighbor IPv6 address.
FiltIn	AS-path filter list applied to input.
FiltOut	AS-path filter list applied to output.
Weight	Neighbor weight value used in BGP best path selection.
RoutemapIn	Neighbor route map applied to input.
RoutemapOut	Neighbor route map applied to output.

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

```
Device# show ipv6 protocols summary

Index Process Name
0     connected
1     static
2     rip myrip
3     bgp 30
```

The following sample output from the **show ipv6 protocols** command displays the EIGRP information including the vector metric and EIGRP IPv6 NSF:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "bgp 1"
  IGP synchronization is disabled
  Redistribution:
    None
IPv6 Routing Protocol is "bgp multicast"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 VR(name) Address-Family Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  NSF-aware route hold timer is 260
  EIGRP NSF enabled
    NSF signal timer is 15s
    NSF converge timer is 65s
  Router-ID: 10.1.2.2
  Topology : 0 (base)
```

```
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 16
      Maximum hopcount 100
      Maximum metric variance 1
      Total Prefix Count: 0
      Total Redist Count: 0

   Interfaces:
   Redistribution:
      None
```

The following example displays IPv6 protocol information after configuring redistribution in an Open Shortest Path First (OSPF) domain:

```
Device# redistribute ospf 1 match internal
Device(config-rtr)# end
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip 1"
  Interfaces:
    Ethernet0/1
    Loopback9
  Redistribution:
    Redistributing protocol ospf 1 (internal)
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0):
    Ethernet0/0
  Redistribution:
    None
```

show ipv6 protocols