show ipv6 rip

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

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

Syntax Description

name	(Optional) Name of the RIP process. If the name is not entered, details of all configured RIP processes will be displayed.
database	(Optional) Details of the entries in the specified RIP IPv6 routing table are displayed.
next-hops	(Optional) Details of the specified RIP IPv6 processes next hop addresses are displayed. If no RIP process name is specified, the next hop addresses for all RIP IPv6 processes will be displayed.

Command Default

Information about all current IPv6 RIP processes is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.2(22)S, and the *name* argument and the **database** and **next-hops** keywords were added.
12.2(13)T	The modifications to add the *name* argument and the **database** and **next-hops** keywords were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

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

```
Router# show ipv6 rip

RIP process "one", port 521, multicast-group FF02::9, pid 55
     Administrative distance is 25. Maximum paths is 4
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
```

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

Table 258 describes the significant fields shown in the display.

Table 258 show ipv6 rip Field Descriptions

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

To display information about a specified IPv6 RIP process database, enter the **show ipv6 rip** command with the *name* argument and the **database** keyword. In the following output for the IPv6 RIP process named one, timer information is displayed, and route 3004::/64 has a route tag set:

```
Router# show ipv6 rip one database

RIP process "one", local RIB
 2001:72D:1000::/64, metric 2
     Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
 2001:72D:2000::/64, metric 2, installed
     Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
 2001:72D:3000::/64, metric 2, installed
```

```
    Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
    Ethernet1/FE80::203:7EBC:FE23:1000, expires in 120 secs
2001:72D:4000::/64, metric 16, expired, [advertise 119/hold 0]
    Ethernet2/FE80::202:7DFF:FE1A:9472
3004::/64, metric 2 tag 2A, installed
    Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
```

Table 259 describes the significant fields shown in the display.

Table 259 show ipv6 rip database Field Descriptions

Field	Description
RIP process	The name of the RIP process.
2001:72D:1000::/64	The IPv6 route prefix.
metric	Metric for the route.
installed	Route is installed in the IPv6 routing table.
Ethernet2/FE80::202:7DFF:FE1A:9472	Interface and LL next hop through which the IPv6 route was learned.
expires in	The interval (in seconds) before the route expires.
advertise	For an expired route, the value (in seconds) during which the route will be advertised as expired.
hold	The value (in seconds) of the hold-down timer.
tag	Route tag.

To display information about the next-hops for a specified IPv6 RIP process, enter the **show ipv6 rip** command with the *name* argument and the **next-hops** keyword:

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

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

Table 260 describes the significant fields shown in the display.

Table 260 show ipv6 rip next-hops Field Descriptions

Field	Description
RIP process	The name of the RIP process.
FE80::210:7BFF:FEC2:ACCF/Ethernet4/2	The next hop address and interface through which it was learned. Next hops are either the addresses of IPv6 RIP neighbors from which we have learned routes, or explicit next hops received in IPv6 RIP advertisements. **Note** An IPv6 RIP neighbor may choose to advertise all its routes with an explicit next hop. In this case the address of the neighbor would not appear in the next hop display.
[1 routes]	The number of routes in the IPv6 RIP routing table using the specified next hop.

show ipv6 route

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

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

Syntax Description

ipv6-address	(Optional) Displays routing information for a specific IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal format using 16-bit values between colons.
ipv6-prefix	(Optional) Displays routing information for a specific IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal format using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays output for longer prefix entries.
protocol	(Optional) Displays routes for the specified routing protocol using any of these keywords: **bgp**, **isis**, **eigrp**, **ospf**, or **rip** or displays routes for the specified type of route using any of these keywords: **connected**, **local**, **mobile**, or **static**.
updated	(Optional) Displays routes with time stamps.
boot-up	(Optional) Displays routing information since the boot up.
day month	(Optional) Displays routes since the day and month specified.
time	(Optional) Displays routes since the time specified. The time is specified in *hh:mm* format.
interface *interface-type*	(Optional) Interface type. For more information about supported interface types, use the question mark (?) online help function.
interface-number	(Optional) Interface number. For more information about the numbering syntax for supported interface types, use the question mark (?) online help function.
nsf	(Optional) Displays routes in the nonstop forwarding state.
table *table-id*	(Optional) Displays IPv6 Routing Information Base (RIB) table information for the specified table ID. The table must be in a hexadecimal format. Range for table ID is 0 to 0-0xFFFFFFFF.
watch	(Optional) Displays information on route watchers.

Command Default

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

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was modified. The **isis** protocol keyword was added to the command syntax, and the I1 - ISIS L1, I2 - ISIS L2, and IA - ISIS interarea fields were 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, the timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T, the timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S. The **longer-prefixes** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **table**, **nsf**, **watch**, and **updated** keywords and *day, month, table-id*, and *time* arguments were added.

Usage Guidelines

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

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

Examples

show ipv6 route Command with No Keyword Specified Example

The following is sample output from the **show ipv6 route** command when entered without an IPv6 address or prefix specified:

```
Router# show ipv6 route
```

```
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   3000::/64 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   4000::2/128 [0/0]
     via ::, Ethernet1/0
C   4000::/64 [0/0]
     via ::, Ethernet1/0
LC  4001::1/128 [0/0]
     via ::, Loopback0
L   5000::2/128 [0/0]
     via ::, Serial6/0
C   5000::/64 [0/0]
     via ::, Serial6/0
S   5432::/48 [1/0]
     via 4000::1, Null
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Table 261 describes the significant fields shown in the display.

Table 261 show ipv6 route Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • C—Connected • L—Local • S—Static • R—RIP derived • B—BGP derived • I1—ISIS L1—Integrated IS-IS Level 1 derived • I2—ISIS L2—Integrated IS-IS Level 2 derived • IA—ISIS interarea—Integrated IS-IS interarea derived
2001:0DB8:DDDD::/32	Indicates the IPv6 prefix of the remote network.
[200/0]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via ::FFFF:192.168.99.70	Specifies the address of the next router to the remote network.
IPv6-mpls	Specifies the interface through which the next router to the specified network can be reached. **Note** In this example output, the interface is the IPv6 Multiprotocol Label Switching (MPLS) virtual interface used in the 6PE feature where IPv6 traffic is sent across an IPv4 MPLS backbone from one IPv6 provider edge router to another.

show ipv6 route Command with Address or Prefix Specified Example

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

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

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

B 2001:200::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

show ipv6 route Command with Protocol Specified Example

When you specify a protocol, only routes for that particular routing protocol are shown. The following is sample output from the **show ipv6 route** command when entered with the **bgp** keyword:

```
Router# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B   3000::/64 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

show ipv6 route Command for Local Routes Example

The following is sample output from the **show ipv6 route** command when entered with the **local** router address:

```
Router# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L   4000::2/128 [0/0]
     via ::, Ethernet1/0
LC  4001::1/128 [0/0]
     via ::, Loopback0
L   5000::2/128 [0/0]
     via ::, Serial6/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

show ipv6 route Command for 6PE Multipath Example'

The following is sample output from the **show ipv6 route** command when used with the 6PE multipath feature enabled:

```
Router# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
.
.
.
B   4004::/64 [200/0]
```

```
via ::FFFF:172.11.11.1
via ::FFFF:172.30.30.1
```

Related Commands

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

show ipv6 route shortcut

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

show ipv6 route shortcut

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ipv6 route shortcut

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

Table 261 describes the significant fields shown in the display.

Table 262 show ipv6 route shortcut Field Descriptions

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

Related Commands

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

show ipv6 route summary

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

show ipv6 route summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

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

```
Router# show ipv6 route summary

IPv6 Routing Table Summary - 257 entries
  37 local, 35 connected, 25 static, 0 RIP, 160 BGP
  Number of prefixes:
    /16: 1, /24: 46, /28: 10, /32: 5, /35: 25, /40: 1, /48: 63, /64: 19
    /96: 15, /112: 1, /126: 31, /127: 4, /128: 36
```

Table 263 describes the significant fields shown in the display.

Table 263 show ipv6 route summary Field Descriptions

Field	Description
entries	Number of entries in the IPv6 routing table.
Route source	Number of routes that are present in the routing table for each route source, which can be local routes, connected routes, static routes, a routing protocol, prefix and address or name, and longer prefixes and address or name. Routing protocols can include RIP, IS-IS, OSPF, and BGP. Other route sources can be connected, local, static, or a specific interface.
Number of prefixes:	Number of routing table entries for given prefix length.

Related Commands

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

show ipv6 route vrf

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

show ipv6 route vrf {*vrf-name* | *vrf-number*}

Syntax Description

vrf-name	Name assigned to the VRF.
vrf-number	Hexadecimal number assigned to the VRF.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

The **show ipv6 route vrf** command displays specified information from the IPv6 routing table of a VRF.

Examples

The following is sample output regarding an IPv6 routing table associated with a VRF named cisco1:

```
Router# show ipv6 route vrf cisco1

IPv6 Routing Table cisco1 - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
C   2001:8::/64 [0/0]
     via ::, FastEthernet0/0
L   2001:8::3/128 [0/0]
     via ::, FastEthernet0/0
B   2002:8::/64 [200/0]
     via ::FFFF:192.168.1.4,
B   2010::/64 [20/1]
     via 2001:8::1,
C   2012::/64 [0/0]
     via ::, Loopback1
L   2012::1/128 [0/0]
     via ::, Loopback1
```

Table 264 describes the significant fields shown in the display.

Table 264 show ipv6 route vrf Field Descriptions

Field	Description
2001:8::/64 [0/0]	Network number.
via ::, FastEthernet0/0	Indicates how the route was derived.

show ipv6 routers

To display IPv6 router advertisement information received from onlink routers, use the **show ipv6 routers** command in user EXEC or privileged EXEC mode.

show ipv6 routers [*interface-type interface-number*] [**conflicts**]

Syntax Description

interface-type	(Optional) Specifies the interface type.
interface-number	(Optional) Specifies the interface number.
conflicts	(Optional) Displays router advertisements that differ from the advertisements configured for a specified interface.

Command Default

When an interface is not specified, onlink router advertisement information is displayed for all interface types. (The term *onlink* refers to a locally reachable address on the link.)

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(2)T	Command output was updated to show the state of the default router preference (DRP) preference value as advertised by other routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Routers advertising parameters that differ from the advertisement parameters configured for the interface on which the advertisements are received are marked as conflicting.

Examples

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

```
Router# show ipv6 routers

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

```
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on Tunnel57, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

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

```
Router# show ipv6 routers

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

Table 265 describes the significant fields shown in the previous two displays.

Table 265 show ipv6 routers Field Descriptions

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

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

```
Router# show ipv6 routers tunnel 5

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

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

```
Router# show ipv6 routers conflicts

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

show ipv6 rpf

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

show ipv6 rpf [**vrf** *vrf-name*] *ipv6-prefix*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-prefix	Summary prefix designated for a range of IPv6 prefixes. The *ipv6-prefix* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ipv6 rpf 2001::1:1:2

RPF information for 2001::1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
  Metric preference:110
```

```
Metric:30
```

Table 266 describes the significant fields shown in the display.

Table 266 show ipv6 rpf Field Descriptions

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

show ipv6 snooping capture-policy

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

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

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ipv6 snooping capture-policy

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

Table 267 describes the significant fields shown in the display.

Table 267 show ipv6 snooping capture-policy Field Descriptions

Field	Description
Hardware policy registered on Fa4/11	A hardware policy contains a programmatic access list (ACL), with a list of access control entries (ACEs).
Protocol	The protocol whose packets are being inspected.
Message	The type of message being inspected.

Table 267 show ipv6 snooping capture-policy Field Descriptions (continued)

Field	Description
Action	Action to be taken on the packet.
Feature	The inspection feature for this information.

show ipv6 snooping counters

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

show ipv6 snooping counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first hop packets that match the specified interface type and number.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

The following examples shows information about packets counted on interface FastEthernet4/12:

```
Router# show ipv6 snooping counters interface Fa4/12

Received messages on Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4256    0       0       0       0       0

Bridged messages from Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4240    0       0       0       0       0

Dropped messages on Fa4/12:
Feature/Message RS      RA      NS      NA      REDIR   CPS     CPA
RA guard        0       16      0       0       0       0       0

Dropped reasons on Fa4/12:
RA guard         16   RA drop - reason:RA/REDIR received on un-authorized port
```

Table 267 describes the significant fields shown in the display.

Table 268 show ipv6 snooping counters Field Descriptions

Field	Description
Received messages on Fa4/12:	The messages received on an interface.
Protocol	The protocol for which messages are being counted.
Protocol message	The type of protocol messages being counted.
Bridged messages from Fa4/12:	Bridged messages from the interface.
Dropped messages an Fa4/12:	The messages dropped on the interface.
Feature/message	The feature that caused the drop, and the type and number of messages dropped.
RA drop - reason:RA/REDIR received on un-authorized port	The reason these messages were dropped.

show ipv6 snooping features

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

show ipv6 snooping features

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ipv6 snooping features

Feature name   priority state
RA guard          100   READY
NDP inspection     20   READY
```

Table 267 describes the significant fields shown in the display.

Table 269 show ipv6 snooping features Field Descriptions

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

show ipv6 snooping policies

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

show ipv6 snooping policies [**interface** *type number*]

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

The following examples shows information about all policies configured:

```
Router# show ipv6 snooping policies

NDP inspection policies configured:

Policy      Interface    Vlan
------      ---------    ----
trusted      Et0/0        all
             Et1/0        all
untrusted    Et2/0        all

RA guard policies configured:

Policy      Interface    Vlan
------      ---------    ----
host         Et0/0        all
             Et1/0        all
router       Et2/0        all
```

Table 267 describes the significant fields shown in the display..

Table 270 show ipv6 first-hop policies Field Descriptions

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

show ipv6 spd

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

show ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ipv6 spd

Current mode: normal
Queue max threshold: 74, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0
```

Table 267 describes the significant fields shown in the display.

Table 271 show ipv6 spd Field Description

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

Related Commands

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

show ipv6 static

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

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

Syntax Description

ipv6-address	(Optional) Provides routing information for a specific IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
ipv6-prefix	(Optional) Provides routing information for a specific IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
interface	(Optional) Name of an interface.
type	(Optional, but required if the **interface** keyword is used) Interface type. For a list of supported interface types, use the question mark (?) online help function.
number	(Optional, but required if the **interface** keyword is used) Interface number. For specific numbering syntax for supported interface types, use the question mark (?) online help function.
recursive	(Optional) Allows the display of recursive static routes only.
detail	(Optional) Specifies the following additional information: • For valid recursive routes, the output path set and maximum resolution depth. • For invalid recursive routes, the reason why the route is not valid. • For invalid direct or fully specified routes, the reason why the route is not valid.

Command Default

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1.0	This command was modified. It was integrated into Cisco IOS XE Release 2.1.0.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.

Usage Guidelines

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

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

Examples

show ipv6 static Command with No Options Specified in the Command Syntax Example

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

```
Router# show ipv6 static

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
  5000::/16, interface Ethernet3/0, distance 1
* 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

Table 272 describes the significant fields shown in the display.

Table 272 show ipv6 static Field Descriptions

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

show ipv6 static Command with the IPv6 Address and Prefix Example

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

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

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

show ipv6 static interface Command Example

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

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

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

show ipv6 static recursive Command Example

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

```
Router# show ipv6 static recursive

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

show ipv6 static detail Command Example

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

- For valid recursive routes, the output path set and maximum resolution depth.
- For invalid recursive routes, the reason why the route is not valid.
- For invalid direct or fully specified routes, the reason why the route is not valid.

```
Router# show ipv6 static detail

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

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ip route	Displays the current state of the routing table.

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

show ipv6 traffic

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

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

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and output fields were added.
12.2(13)T	The modification to add output fields was integrated into this release.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	The *interface* argument and **interface** keyword were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

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

Examples

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

```
Router# show ipv6 traffic

IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
```

```
          0 bad header, 0 unknown option, 0 bad source
          0 unknown protocol, 0 not a router
          0 fragments, 0 total reassembled
          0 reassembly timeouts, 0 reassembly failures
          0 unicast RPF drop, 0 suppressed RPF drop
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
```

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

```
Router# show ipv6 interface ethernet 0/1/1

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

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

```
Router# show ipv6 interface ethernet 0/1/1

Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
```

```
    Process Switching:
      0 verification drops
      0 suppressed verification drops
    CEF Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

Table 273 describes the significant fields shown in the display.

Table 273 show ipv6 traffic Field Descriptions

Field	Description
source-routed	Number of source-routed packets.
truncated	Number of truncated packets.
format errors	Errors that can result from checks performed on header fields, the version number, and packet length.
not a router	Message sent when IPv6 unicast routing is not enabled.
0 unicast RPF drop, 0 suppressed RPF drop	Number of unicast and suppressed reverse path forwarding (RPF) drops.
failed	Number of failed fragment transmissions.
encapsulation failed	Failure that can result from an unresolved address or try-and-queue packet.
no route	Counted when the software discards a datagram it did not know how to route.
unreach	Unreachable messages received are as follows: • routing—Indicates no route to the destination. • admin—Indicates that communication with the destination is administratively prohibited. • neighbor—Indicates that the destination is beyond the scope of the source address. For example, the source may be a local site or the destination may not have a route back to the source. • address—Indicates that the address is unreachable. • port—Indicates that the port is unreachable.
Unicast RPF access-list MINI	Unicast RPF access-list in use.
Process Switching	Displays process RPF counts, such as verification and suppressed verification drops.
CEF Switching	Displays CEF switching counts, such as verification drops and suppressed verification drops.

show ipv6 tunnel

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

show ipv6 tunnel

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

Examples

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

```
Router# show ipv6 tunnel

Tun Route  LastInp  Packets
  0 RIPng    never        0
  1   -   00:00:13    55495
  2   -      never        0
  3   -   00:00:21    14755
  4   -      never        0
  5   -   00:00:00    15840
  6   -      never        0
  7   -   00:00:18    16008
  8   -      never        0
  9   -      never        0
 10   -      never        0
 11   -   00:00:03    94801
 12   -      1d02h        2
 13   -      never        0
 14   -   00:00:08   312190
```

```
15   -      never        0
16   -      never        0
17   -      never        0
18   -   00:00:05  1034954
19   -      never        0
20   -   00:00:01  1171114
21   -      never        0
```

Table 274 describes the significant fields shown in the display.

Table 274 show ipv6 tunnel Field Descriptions

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

show ipv6 virtual-reassembly

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

show ipv6 virtual-reassembly interface *interface-type*

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ipv6 virtual-reassembly

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

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

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

Related Commands

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

show ipv6 virtual-reassembly features

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

The following example displays information about all interfaces:

```
Router# show ipv6 virtual-reassembly features

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

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

Related Commands

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

show isis database

To display the Intermediate System-to-Intermediate System (IS-IS) link-state database, use the **show isis database** command in user EXEC or privileged EXEC mode.

show isis [*process-tag*] **database** [**level-1** | **l1**] [**level-2** | **l2**][**detail**] [**lspid**]

Syntax Description

process-tag	(Optional) A unique name among all International Organization for Standardization (ISO) router processes including IP and Connectionless Network Service (CLNS) router processes for a given router. If a process tag is specified, output is limited to the specified routing process. When **null** is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.
level-1	(Optional) Displays the IS-IS link-state database for Level 1. l1 is the abbreviation for the **level-1** keyword
level-2	(Optional) Displays the IS-IS link-state database for Level 2. l2 is the abbreviation for the **level-2** keyword.
detail	(Optional) Displays the contents of each link-state packet (LSP). Otherwise, a summary display is provided.
lspid	(Optional) Displays the link-state protocol data unit (PDU) identifier. Displays the contents of a single LSP by its ID number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(15)T	Support was added for IPv6.
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(29)S	The *process-tag* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)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 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The order of the optional argument and keywords is not important when this command is entered. For example, the following are both valid command specifications and provide the same output: **show isis database detail l2** and **show isis database l2 detail**.

Examples

The following is sample output from the **show isis database** command:

```
Router# show isis database

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num    LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C     0x5696        792           0/0/0
0000.0C00.40AF.00-00* 0x00000009     0x8452        1077          1/0/0
0000.0C00.62E6.00-00  0x0000000A     0x38E7        383           0/0/0
0000.0C00.62E6.03-00  0x00000006     0x82BC        384           0/0/0
0800.2B16.24EA.00-00  0x00001D9F     0x8864        1188          1/0/0
0800.2B16.24EA.01-00  0x00001E36     0x0935        1198          1/0/0

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num    LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.03-00  0x00000005     0x04C8        792           0/0/0
0000.0C00.3E51.00-00  0x00000007     0xAF96        758           0/0/0
0000.0C00.40AF.00-00* 0x0000000A     0x3AA9        1077          0/0/0
```

The following is sample output from the **show isis database** command using the *process-tag* argument to display information about a VPN routing and forwarding instance (VRF)-aware IS-IS instance tagFirst:

```
Router# show isis tagFirst database level-2

Tag tagFirst:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num    LSP Checksum  LSP Holdtime  ATT/P/OL
igp-01.00-00          0x0000000A     0x5E73        914           0/0/0
igp-01.03-00          0x00000001     0x8E41        894           0/0/0
igp-01.04-00          0x00000001     0x8747        894           0/0/0
igp-03.00-00        * 0x00000005     0x55AD        727           0/0/0
igp-03.02-00        * 0x00000001     0x3B97        727           0/0/0
igp-02.00-0           0x00000004     0xC1FB        993           0/0/0
igp-02.01-00          0x00000001     0x448D        814           0/0/0
igp-04.00-00          0x00000004     0x76D0        892           0/0/0
```

Table 275 describes the significant fields shown in the display.

Table 275 show isis database Field Descriptions

Field	Description
Tag tagFirst	Tag name that identifies an IS-IS instance.
LSPID	The LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is nonzero, the LSP describes links from the system. When it is zero, the LSP is a so-called nonpseudonode LSP. This mechanism is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP will describe the state of the originating router. For each LAN, the designated router for that LAN will create and flood a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP will be divided into multiple LSP fragments. Each fragment will have a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.

Table 275 show isis database Field Descriptions (continued)

Field	Description
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP will stay in the LSDB before being completely removed.
ATT	The Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers will use the Attach bit to find the closest Level 2 router. They will point a default route to the closest Level 2 router.
P	The P bit. Detects if the intermediate systems is area partition repair-capable. Cisco and other vendors do not support area partition repair.
OL	The Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers will not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router will be sent to this router.

The following is sample output from the **show isis database detail** command:

```
Router# show isis database detail

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C   0x5696        325           0/0/0
  Area Address: 47.0004.004D.0001
  Area Address: 39.0001
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.0C35
0000.0C00.40AF.00-00* 0x00000009   0x8452        608           1/0/0
  Area Address: 47.0004.004D.0001
  Topology: IPv4 (0x0) IPv6 (0x2)
  NLPID: 0xCC 0x8E
  IP Address: 172.16.21.49
  Metric: 10   IS 0800.2B16.24EA.01
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.40AF
  IPv6 Address: 2001:0DB8::/32
  Metric: 10   IPv6 (MT-IPv6) 2001:0DB8::/64
  Metric: 5    IS-Extended cisco.03
  Metric: 10   IS-Extended cisco1.03
  Metric: 10    IS (MT-IPv6) cisco.03
```

As the output shows, in addition to the information displayed with the **show isis database** command, the **show isis database detail** command displays the contents of each LSP.

Table 276 describes the significant fields shown in the display.

Table 276 show isis database detail Field Descriptions

Field	Description
Area Address	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system [ES], or a CLNS prefix).
Topology	States the topology supported (for example, IPv4, IPv6).
IPv6 Address	The IPv6 address.
MT-IPv6	Advertised using multitopology Type, Length, and Value objects (TLVs).

The following is additional sample output from the **show isis database detail** command. This LSP is a Level 2 LSP. The area address 39.0001 is the address of the area in which the router resides.

```
Router# show isis database 12 detail

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.1111.00-00* 0x00000006   0x4DB3        1194          0/0/0
  Area Address: 39.0001
  NLPID:       0x81 0xCC
  IP Address:  172.16.64.17
  Metric: 10   IS 0000.0C00.1111.09
  Metric: 10   IS 0000.0C00.1111.08
  Metric: 10   IP 172.16.65.0 255.255.255.0
```

show isis ipv6 rib

To display the IPv6 local Routing Information Base (RIB), use the **show isis ipv6 rib** command in user EXEC or privileged EXEC mode.

show isis ipv6 rib [*ipv6-prefix*]

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

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

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

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

Examples

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

```
Router# show isis ipv6 rib

IS-IS IPv6 process "", local RIB
  88:1::/64
    via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2  metric 20 LSP [3/7]
* 1357:1::/64
    via FE80::202:7DFF:FE1A:9471/Ethernet2/1, type L2  metric 10 LSP [4/9]
* 2001:45A::/64
```

```
via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L1  metric 20 LSP [C/6]
via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L1  metric 20 LSP [C/6]
via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2  metric 20 LSP [3/7]
via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2  metric 20 LSP [3/7]
```

Table 277 describes the significant fields shown in the display.

Table 277 show isis ipv6 rib Field Descriptions

Field	Description
*	Prefixes that have been installed in the master IPv6 RIB as IS-IS routes.
type	Type of path: • L1—Level 1 • L2—Level 2 • IA—Inter-area • Sum—Summary
LSP [3/7]	Link-state packet (LSP). The numbers following LSP indicate the LSP index and LSP version, respectively.

show isis spf-log

To display how often and why the router has run a full shortest path first (SPF) calculation, use the **show isis spf-log** command in privileged EXEC mode.

show isis [*area-tag*] [**ipv6** | *] **spf-log** [**topology** {**ipv6** | *topology-name* | *}]

Syntax Description

area-tag	(Optional) Required for multiarea Intermediate System-to-Intermediate System (IS-IS) configuration. Optional for conventional IS-IS configuration. Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.
ipv6	(Optional) Displays the IS-IS multitopology for IPv6 SPF log.
*	(Optional) Displays the SPF logs of all address families.
topology	(Optional) Specifies the Multiple Transport Stream Receiver (MTR) topology.
topology-name	(Optional) The IS-IS multitopology SPF log for the specified topology name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(15)T	Support was added for IPv6.
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(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 2.4	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show isis spf-log** command with the optional **ipv6** keyword:

```
Router# show isis ipv6 spf-log

                   IPv6 Level 1 SPF log
  When   Duration  Nodes  Count     Last trigger LSP   Triggers
00:15:46    3124     40      1          milles.00-00  TLVCODE
00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP
00:15:19    3096     41      1          deurze.00-00  TLVCODE
```

```
00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER
00:14:49    3384     41      1          milles.00-01  TLVCODE
00:14:23    2932     41      3          milles.00-00  TLVCODE
00:05:18    3140     41      1                        PERIODIC
00:03:54    3144     41      1          milles.01-00  TLVCODE
00:03:49    2908     41      1          milles.01-00  TLVCODE
00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT
00:03:15    3054     41      1          milles.00-00  TLVCODE
00:02:53    2958     41      1          mortel.00-00  TLVCODE
00:02:48    3632     41      2          milles.00-00  NEWADJ TLVCODE
00:02:23    2988     41      1          milles.00-01  TLVCODE
00:02:18    3016     41      1          gemert.00-00  TLVCODE
00:02:14    2932     41      1           bakel.00-00  TLVCONTENT
00:02:09    2988     41      2           bakel.00-00  TLVCONTENT
00:01:54    3228     41      1          milles.00-00  TLVCODE
00:01:38    3120     41      3            rips.03-00  TLVCONTENT
```

Table 278 describes the significant fields shown in the display.

Table 278 show isis spf-log Field Descriptions

Field	Description
When	How long ago (in hours: minutes: seconds) a full SPF calculation occurred. The last 20 occurrences are logged.
Duration	Number of milliseconds required to complete this SPF run. Elapsed time is wall clock time, not CPU time.
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. A router waits 5 seconds before running a full SPF run, so it can include all new information. This count denotes the number of events (such as receiving new LSPs) that occurred while the router was waiting its 5 seconds before running full SPF.
Last trigger LSP	Whenever a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue as to the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the last received LSP is remembered.
Triggers	A list of all reasons that triggered a full SPF calculation. For a list of possible triggers, see Table 279.

Table 279 lists possible triggers of a full SPF calculation.

Table 279 Possible Triggers of Full SPF Calculation

Trigger	Description
ADMINDIST	Another administrative distance was configured for the IS-IS process on this router.
AREASET	Set of learned area addresses in this area changed.
ATTACHFLAG	This router is now attached to the Level 2 backbone or it has just lost contact to the Level 2 backbone.

Table 279 Possible Triggers of Full SPF Calculation (continued)

Trigger	Description
BACKUPOVFL	An IP prefix disappeared. The router knows there is another way to reach that prefix but has not stored that backup route. The only way to find the alternative route is through a full SPF run.
DBCHANGED	A **clear isis *** command was issued on this router.
IPBACKUP	An IP route disappeared, which was not learned via IS-IS, but via another protocol with better administrative distance. IS-IS will run a full SPF to install an IS-IS route for the disappeared IP prefix.
IPQUERY	A **clear ip route** command was issued on this router.
LSPEXPIRED	Some LSP in the link-state database (LSDB) has expired.
LSPHEADER	ATT/P/OL bits or is-type in an LSP header changed.
NEWADJ	This router has created a new adjacency to another router.
NEWAREA	A new area (via network entity title [NET]) was configured on this router.
NEWLEVEL	A new level (via is-type) was configured on this router.
NEWLSP	A new router or pseudonode appeared in the topology.
NEWMETRIC	A new metric was configured on an interface of this router.
NEWSYSID	A new system ID (via NET) was configured on this router.
PERIODIC	Typically, every 15 minutes a router runs a periodic full SPF calculation.
RTCLEARED	A **clear clns route** command was issued on this router.
TLVCODE	TLV code mismatch, indicating that different type length values (TLVs) are included in the newest version of an LSP.
TLVCONTENT	TLV contents changed. This normally indicates that an adjacency somewhere in the area has come up or gone down. The “Last trigger LSP” column indicates where the instability may have occurred.

show isis topology

To display a list of all connected routers in all areas, use the **show isis topology** command in user EXEC or privileged EXEC mode.

show isis [*process-tag*] [**ipv6** | *] **topology** [*hostname*] [**level-1** | **level-2** | **l1** | **l2**]

Syntax Description

process-tag	(Optional) A unique name among all International Organization for Standardization (ISO) router processes including IP and Connectionless Network Service (CLNS) router processes for a given router. If a process tag is specified, output is limited to the specified routing process. When **null** is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.
ipv6	(Optional) Displays Intermediate System-to-Intermediate System (IS-IS) IPv6 topology.
*	(Optional) Displays the topology of all address families.
hostname	(Optional) Hostname or the Network Service Access Point (NSAP) address of the router.
level-1	(Optional) Specifies paths to all level one routers in the area.
level-2	(Optional) Specifies paths to all level two routers in the domain.
l1	(Optional) Abbreviation for the **level-1** keyword.
l2	(Optional) Abbreviation for the **level-2** keyword.

Command Modes

Privileged EXEC (#)

Command History

OS Release	Modification
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.0(29)S	This command was modified. The *process-tag* argument was added.
S Release	**Modification**
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
SB Release	**Modification**
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
SG Release	**Modification**
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
SX Release	**Modification**
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Mainline and T Release	**Modification**
12.0(5)T	This command was introduced.
12.2(15)T	This command was modified. Support was added for IPv6.
XE Release	**Modification**
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **show isis topology** command to verify the presence and connectivity between all routers in all IS-IS areas.

If you are running Cisco IOS Release 12.2(33)SRB or a later release, use the **show isis topology** (MTR) command.

Examples

The following is sample output from the **show isis topology** command using the optional **ipv6** keyword. The command shown is used in a dual CLNS-IP network:

```
Router# show isis ipv6 topology

Tag L2BB:
IS-IS IPv6 paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0005 --
0000.0000.0009  10      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0017  20      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0053  30      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0068  20      0000.0000.0009  Tu529           *Tunnel*

IS-IS paths to level-2 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0005  --
0000.0000.0009  10      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0017  20      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0053  30      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0068  20      0000.0000.0009  Tu529           *Tunnel*
Tag A3253-01:
IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0003  10      0000.0000.0003  Et1             0000.0c03.6944
0000.0000.0005  --
```

```
0000.0000.0053  10      0000.0000.0053  Et1             0060.3e58.ccdb

Tag A3253-02:
IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0002  10      0000.0000.0002  Et2             0000.0c03.6bc5
0000.0000.0005  --
0000.0000.0053  10      0000.0000.0053  Et2             0060.3e58.ccde
```

Table 280 describes the significant fields shown in the display.

Table 280 show isis topology Field Descriptions

Field	Description
Tag	Identifies the routing process.
System Id	Six-byte value that identifies a system in an area.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system [ES], or a CLNS prefix).
Next-Hop	The address of the next hop router.
Interface	Interface from which the system was learned.
SNPA	Subnetwork point of attachment. This is the data-link address.

Related Commands

Command	Description
show clns es-neighbors	Lists the ES neighbors that this router knows.
show clns is-neighbors	Displays IS-IS related information for IS-IS router adjacencies.
show clns neighbors	Displays the ES, IS, and M-ISIS neighbors.
show clns neighbor areas	Displays information about IS-IS neighbors and the areas to which they belong.
show clns route	Displays one or all of the destinations to which the router knows how to route CLNS packets.

show key chain

To display authentication key information, use the **show key chain** command in EXEC mode.

show key chain [*name-of-chain*]

Syntax Description

name-of-chain	(Optional) Name of the key chain to display, as named in the **key chain** command.

Defaults

Information about all key chains is displayed.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show key chain** command:

```
Router# show key chain

Key-chain trees:
    key 1 -- text "chestnut"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
    key 2 -- text "birch"
        accept lifetime (00:00:00 Dec 5 1995) - (23:59:59 Dec 5 1995)
        send lifetime (06:00:00 Dec 5 1995) - (18:00:00 Dec 5 1995)
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

show l2tp session

To display information about Layer 2 Tunneling Protocol (L2TP) sessions, use the **show l2tp session** command in privileged EXEC mode.

show l2tp session [**all** | **packets** [**ipv6**] | **sequence** | **state** | [**brief** | **circuit** | **interworking**] [**hostname**]] [**ip-addr** *ip-addr* [**vcid** *vcid*] | **tunnel** {**id** *local-tunnel-id local-session-id* | **remote-name** *remote-tunnel-name local-tunnel-name*} | **username** *username* | **vcid** *vcid*]

Syntax Description

all	(Optional) Displays information for all active sessions.
packets	(Optional) Displays information about packet or byte counts for sessions.
ipv6	(Optional) (Optional) Displays IPv6 packet and byte-count statistics.
sequence	(Optional) Displays sequence information for sessions.
state	(Optional) Displays state information for sessions.
brief	(Optional) Displays brief session information.
circuit	(Optional) Displays the Layer 2 circuit information.
interworking	(Optional) Displays interworking information.
hostname	(Optional) Displays output using L2TP control channel hostnames rather than IP addresses
ip-addr *ip-addr*	(Optional) Specifies the peer IP address associated with the session.
vcid *vcid*	(Optional) Specifies the Virtual Circuit ID (VCID) associated with the session. The range is from 1 to 4294967295.
tunnel	(Optional) Displays the sessions in a tunnel.
id *local-tunnel-id local-session-id*	Specifies the session by tunnel ID and session ID. The range for the local tunnel ID and local session ID is from 1 to 4294967295.
remote-name *remote-tunnel-name local-tunnel-name*	Specifies the remote names for the remote and local L2TP tunnels.
username *username*	(Optional) Specifies the username associated with the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show l2tp session** command with the **all** keyword was modified to display IPv6 counter information.

Usage Guidelines

To use the **show l2tp session** command, you must configure the following commands:

- The **vpdn enable** command in global configuration mode
- The **vpdn-group** command in global configuration mode
- The **request-dialin** command in VPDN group configuration mode
- The **protocol** command in request dial-in VPDN subgroup configuration mode
- The **domain** command in request dial-in VPDN subgroup configuration mode
- The **initiate-to** command in VPDN group configuration mode
- The **local name** command in VPDN group configuration mode
- The **l2tp tunnel password** command in VPDN group configuration mode
- The **l2tp attribute clid mask-method** command in VPDN group configuration mode

Examples

The following is sample output from the **show l2tp session** command:

```
Router# show l2tp session packets

L2TP Session Information Total tunnels 1 sessions 2

LocID      RemID      TunID      Pkts-In    Pkts-Out   Bytes-In   Bytes-Out
18390      313101640  4059745793 0          0          0          0
25216      4222832574 4059745793 15746      100000     1889520    12000000
```

Related Commands

Command	Description
domain (isakmp-group)	Specifies the DNS domain to which a group belongs and enters the ISAKMP group configuration mode.
initiate-to	Specifies an IP address used for Layer 2 tunneling.
local name	Specifies a local hostname that the tunnel uses to identify itself.
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template and enters a VPDN group or VPDN template configuration mode.
l2tp tunnel password	Sets the password the router uses to authenticate L2TP tunnels.
protocol (L2TP)	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show l2tp tunnel

To display details about Layer 2 Tunneling Protocol (L2TP) tunnels, use the **show l2tp tunnel** command in privileged EXEC mode.

show l2tp tunnel [**all** | **packets** [**ipv6**] | **state** | **summary** | **transport**] [**id** *local-tunnel-id* | **local-name** *local-tunnel-name remote-tunnel-name* | **remote-name** *remote-tunnel-name local-tunnel-name*]

Syntax Description

all	(Optional) Displays information about all active tunnels.
packets	(Optional) Displays information about packet or byte counts.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
state	(Optional) Displays the state of the tunnel.
summary	(Optional) Displays a summary of the tunnel information.
transport	(Optional) Displays tunnel transport information.
id *local-tunnel-id*	(Optional) Specifies the local tunnel ID of the L2TP tunnel. The range is from 1 to 4294967295.
local-name *local-tunnel-name remote-tunnel-name*	(Optional) Specifies the local names for the local and remote L2TP tunnels.
remote-name *remote-tunnel-name local-tunnel-name*	(Optional) Specifies the remote names for the remote and local L2TP tunnels.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show l2tp tunnel** command with the **all** keyword was modified to display IPv6 counter information.

Usage Guidelines

To use the **show l2tp tunnel** command, you must configure the following commands:

- The **vpdn enable** command in global configuration mode
- The **vpdn-group** command in global configuration mode
- The **request-dialin** command in VPDN group configuration mode
- The **protocol** command in request dial-in VPDN subgroup configuration mode
- The **domain** command in request dial-in VPDN subgroup configuration mode

- The **initiate-to** command in VPDN group configuration mode
- The **local name** command in VPDN group configuration mode
- The **l2tp tunnel password** command in VPDN group configuration mode
- The **l2tp attribute clid mask-method** command in VPDN group configuration mode

Depending on the keywords or arguments entered, the **show l2tp tunnel** command displays information such as packet or byte count, state, transport, local or remote names, and summary information for L2TP tunnels.

Examples

The following is sample output from the **show l2tp tunnel** command:

```
Router# show l2tp tunnel all

L2TP Tunnel Information Total tunnels 1 sessions 1 Tunnel id 746420372 is up, remote id is
2843347489, 1 active sessions
 Remotely initiated tunnel
 Tunnel state is established, time since change 00:30:16  Tunnel transport is IP (115)
 Remote tunnel name is 7604-AA1705
  Internet Address 12.27.17.86, port 0
 Local tunnel name is 7606-AA1801
  Internet Address 12.27.18.86, port 0
 L2TP class for tunnel is l2tp_default_class
 Counters, taking last clear into account:
  598 packets sent, 39 received
  74053 bytes sent, 15756 received
  Last clearing of counters never
 Counters, ignoring last clear:
  598 packets sent, 39 received
  74053 bytes sent, 15756 received
 Control Ns 3, Nr 35
 Local RWS 1024 (default), Remote RWS 1024
 Control channel Congestion Control is disabled
 Tunnel PMTU checking disabled
 Retransmission time 1, max 1 seconds
 Unsent queuesize 0, max 0
 Resend queuesize 0, max 1
 Total resends 0, ZLB ACKs sent 33
 Total out-of-order dropped pkts 0
 Total out-of-order reorder pkts 0
 Total peer authentication failures 0
 Current no session pak queue check 0 of 5
 Retransmit time distribution: 0 0 0 0 0 0 0 0 0
 Control message authentication is disabled
```

Related Commands

Command	Description
domain (isakmp-group)	Specifies the DNS domain to which a group belongs and enters the ISAKMP group configuration mode.
initiate-to	Specifies an IP address used for Layer 2 tunneling.
local name	Specifies a local hostname that the tunnel uses to identify itself.
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template and enters a VPDN group or VPDN template configuration mode.
l2tp tunnel password	Sets the password the router uses to authenticate L2TP tunnels.

Command	Description
protocol (L2TP)	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show l2tun session

To display the current state of Layer 2 sessions and protocol information about Layer 2 Tunnel Protocol (L2TP) control channels, use the **show l2tun session** command in privileged EXEC mode.

show l2tun session [**l2tp** | **pptp**] [**all** [*filter*] | **brief** [*filter*] [**hostname**] | **circuit** [*filter*] [**hostname**] | **interworking** [*filter*] [**hostname**] | **packets** [**ipv6**] [*filter*] | **sequence** [*filter*] | **state** [*filter*]]

Syntax Descriptions

l2tp	(Optional) Displays information about L2TP.
pptp	(Optional) Displays information about Point-to-Point Tunneling Protocol.
all	(Optional) Displays information about all current L2TP sessions on the router.
filter	(Optional) One of the filter parameters defined in Table 281.
brief	(Optional) Displays information about all current L2TP sessions, including the peer ID address and circuit status of the L2TP sessions.
hostname	(Optional) Specifies that the peer hostname will be displayed in the output.
circuit	(Optional) Displays information about all current L2TP sessions, including circuit status (up or down).
interworking	(Optional) Displays information about Layer 2 Virtual Private Network (L2VPN) interworking.
packets	(Optional) Displays information about the packet counters (in and out) associated with current L2TP sessions.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
sequence	(Optional) Displays sequencing information about each L2TP session, including the number of out-of-order and returned packets.
state	(Optional) Displays information about all current L2TP sessions and their protocol state, including remote Virtual Connection Identifiers (VCIDs).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(31)S	The **hostname** keyword was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(22)T	This command was modified.The **pptp** and **tunnel** keywords were added.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show l2tun session** command with the **all** and **l2tp all** keywords was modified to display IPv6 counter information.

Usage Guidelines

Use the **show l2tun session** command to display information about current L2TP sessions on the router.

Table 281 defines the filter parameters available to refine the output of the **show l2tun session** command.

Table 281 Filter Parameters for the show l2tun session Command

Syntax	Description
ip-addr *ip-address* [**vcid** *number*]	Filters the output to display information about only those L2TP sessions associated with the IP address of the peer router. The 32-bit VCID shared between the peer router and the local router at each end of the control channel can be optionally specified. • *ip-address*—IP address of the peer router. • *number*—VCID number.
vcid *number*	Filters the output to display information about only those L2TP sessions associated with the VCID shared between the peer router and the local router at each end of the control channel. • *number*—VCID number.
username *username*	Filters the output to display information for only those sessions associated with the specified username. • *username*—Username.
tunnel {**id** *local-tunnel local-session* | **remote-name** *remote-tunnel local-tunnel-name*}	Displays the sessions in a tunnel. • **id**—Tunnel ID for established tunnels. • *local-tunnel*—Local tunnel ID. • *local-session*—Local session ID. • **remote-name**—Remote tunel name. • *remote-tunnel*—Remote tunnel name. • *local-tunnel*—Local tunnel name.

Examples

The following example shows how to display detailed information about all current L2TP sessions:

```
Router# show l2tun session all

Session Information Total tunnels 0 sessions 1

Session id 42438 is down, tunnel id n/a
  Remote session id is 0, remote tunnel id n/a
Session Layer 2 circuit, type is Ethernet, name is FastEthernet4/1/1
  Session vcid is 123456789
  Circuit state is DOWN
    Local circuit state is DOWN
    Remote circuit state is DOWN
Call serial number is 1463700128
Remote tunnel name is PE1
  Internet address is 10.1.1.1
Local tunnel name is PE1
  Internet address is 10.1.1.2
IP protocol 115
  Session is L2TP signalled
  Session state is idle, time since change 00:00:26
    0 Packets sent, 0 received
```

```
    0 Bytes sent, 0 received
  Last clearing of "show vpdn" counters never
    Receive packets dropped:
      out-of-order:            0
      total:                   0
    Send packets dropped:
      exceeded session MTU:    0
      total:                   0
  DF bit off, ToS reflect disabled, ToS value 0, TTL value 255
  No session cookie information available
  UDP checksums are disabled
  L2-L2 switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 1
```

The following example shows how to display information only about the L2TP session set up on a peer router with an IP address of 192.0.2.0 and a VCID of 300:

```
Router# show l2tun session all ip-addr 192.0.2.0 vcid 300

L2TP Session
Session id 32518 is up, tunnel id n/a
Call serial number is 2074900020
Remote tunnel name is tun1
  Internet address is 192.0.2.0
Session is L2TP signalled
  Session state is established, time since change 03:06:39
    9932 Packets sent, 9932 received
    1171954 Bytes sent, 1171918 received
  Session vcid is 300
  Session Layer 2 circuit, type is Ethernet Vlan, name is FastEthernet0/1/0.3:3
  Circuit state is UP
    Remote session id is 18819, remote tunnel id n/a
  Set DF bit to 0
  Session cookie information:
    local cookie, size 4 bytes, value CF DC 5B F3
    remote cookie, size 4 bytes, value FE 33 56 C4
  SSS switching enabled
  Sequencing is on
    Ns 9932, Nr 10001, 0 out of order packets discarded
```

Table 282 describes the significant fields shown in the displays.

Table 282 show l2tun session Field Descriptions

Field	Description
Total tunnels	Total number of L2TP tunnels established on the router.
sessions	Number of L2TP sessions established on the router.
Session id	Session ID for established sessions.
is	Session state.
tunnel id	Tunnel ID for established tunnels.
Remote session id	Session ID for the remote session.
tunnel id	Tunnel ID for the remote tunnel.
Session Layer 2 circuit, type is, name is	Type and name of the interface used for the Layer 2 circuit.

Table 282 show l2tun session Field Descriptions (continued)

Field	Description
Session vcid is	VCID of the session.
Circuit state is	State of the Layer 2 circuit.
Local circuit state is	State of the local circuit.
Remote circuit state is	State of the remote circuit.
Call serial number is	Call serial number.
Remote tunnel name is	Name of the remote tunnel.
Internet address is	IP address of the remote tunnel.
Local tunnel name is	Name of the local tunnel.
Internet address is	IP address of the local tunnel.
IP protocol	The IP protocol used.
Session is	Signaling type for the session.
Session state is	Session state for the session.
time since change	Time since the session state last changed, in the format hh:mm:ss.
Packets sent, received	Number of packets sent and received since the session was established.
Bytes sent, received	Number of bytes sent and received since the session was established.
Last clearing of "show vpdn" counters	Time elapsed since the last clearing of the counters displayed with the **show vpdn** command. Time will be displayed in one of the following formats: • hh:mm:ss—Hours, minutes, and seconds. • dd:hh—Days and hours. • WwDd—Weeks and days, where W is the number of weeks and D is the number of days. • YyWw—Years and weeks, where Y is the number of years and W is the number of weeks. • never—The timer has not been started.
Receive packets dropped:	Number of received packets that were dropped since the session was established. • out-of-order—Total number of received packets that were dropped because they were out of order. • total—Total number of received packets that were dropped.
Send packets dropped:	Number of sent packets that were dropped since the session was established. • exceeded session MTU—Total number of sent packets that were dropped because the session maximum transmission unit (MTU) was exceeded. • total—Total number of sent packets that were dropped.
DF bit	Status of the Don't Fragment (DF) bit option. The DF bit can be on or off.
ToS reflect	Status of the type of service (ToS) reflect option. ToS reflection can be enabled or disabled.
ToS value	Value of the ToS byte in the L2TP header.

Table 282 show l2tun session Field Descriptions (continued)

Field	Description
TTL value	Value of the time-to-live (TTL) byte in the L2TP header.
local cookie	Size (in bytes) and value of the local cookie.
remote cookie	Size (in bytes) and value of the remote cookie.
UDP checksums are	Status of the User Datagram Protocol (UDP) checksum configuration.
switching	Status of switching.
No FS cached header information available	Fast Switching (FS) cached header information. If an FS header is configured, the encapsulation size and hexadecimal contents of the FS header will be displayed. The FS header is valid only for IP virtual private dialup network (VPDN) traffic from a tunnel server to a network access server (NAS).
Sequencing is	Status of sequencing. Sequencing can be on or off.
Ns	Sequence number for sending.
Nr	Sequence number for receiving.
Unique ID is	Global user ID correlator.

The following example shows how to display information about the circuit status of L2TP sessions on a router:

```
Router# show l2tun session circuit

Session Information Total tunnels 3 sessions 3

LocID      TunID      Peer-address    Type Stat Username, Intf/
                                               Vcid, Circuit
32517      n/a         172.16.184.142  VLAN UP   100, Fa0/1/0.1:1
32519      n/a         172.16.184.142  VLAN UP   200, Fa0/1/0.2:2
32518      n/a         172.16.184.142  VLAN UP   300, Fa0/1/0.3:3
```

The following example shows how to display information about the circuit status of L2TP sessions and the hostnames of remote peers:

```
Router# show l2tun session circuit hostname

Session Information Total tunnels 3 sessions 3

LocID      TunID      Peer-hostname Type Stat Username, Intf/
                                               Vcid, Circuit
32517      n/a         <unknown>       VLAN UP   100, Fa0/1/0.1:1
32519      n/a         router32        VLAN UP   200, Fa0/1/0.2:2
32518      n/a         access3         VLAN UP   300, Fa0/1/0.3:3
```

Table 283 describes the significant fields shown in the displays.

Table 283 show l2tun session circuit Field Descriptions

Field	Description
LocID	Local session ID.
TunID	Tunnel ID.
Peer-address	IP address of the peer.
Peer-hostname	Hostname of the peer.

Table 283 show l2tun session circuit Field Descriptions (continued)

Field	Description
Type	Session type.
Stat	Session status.
Username, Intf/Vcid, Circuit	Username, interface name/VCID, and circuit number of the session.

Related Commands

Command	Description
show l2tun	Displays general information about Layer 2 tunnels and sessions.
show l2tun tunnel	Displays the current state of Layer 2 tunnels and information about configured tunnels.

show mls cef ipv6

To display the hardware IPv6-switching table entries, use the **show mls cef ipv6** command in privileged EXEC mode.

show mls cef ipv6 [**vrf** *vrf-name*] [*ip-address/mask*] [**accounting per-prefix**] [**module** *number*]

show mls cef ipv6 exact-route *src-addr* [*L4-src-port*] *dst-addr* [*L4-dst-port*]

show mls cef ipv6 multicast tcam [*v6mcast-address*] [**detail**] [**internal**]

Syntax Description

vrf	(Optional) IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name.
ip-address/mask	(Optional) Entry IPv6 address and prefix mask. Valid values for the *mask* argument are from 0 through 128.
accounting per-prefix	(Optional) Displays per-prefix accounting statistics.
module *number*	(Optional) Displays the entries for a specific module.
exact-route	Provides the exact route of IPv6-switching table entries.
src-addr	Source IP address.
L4-src-port	(Optional) Layer 4-source port number; valid values are from 0 to 65535.
dst-addr	Destination IP address.
L4-dst-port	(Optional) Layer 4-destination port number; valid values are from 0 to 65535.
multicast tcam	Displays IPv6-multicast entries.
v6mcast-address	(Optional) IPv6-multicast address.
detail	(Optional) Displays detailed hardware information.
internal	(Optional) *Displays internal hardware information.*

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	The output was changed to display multicast protocol information in the Forwarding Information Base (FIB) driver.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

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

You can enter this command on the supervisor engine and Multilayer Switching (MLS)-hardware Layer 3-switching module consoles only. Enter the **remote login** command to enter a session into the supervisor engine and distributed forwarding card (DFC)-equipped module to enter the commands.

When entering the *ip-address/mask* argument, use this format, X:X:X:X::X/*mask,* where valid values for *mask* are from 0 to 128.

Up to 64 IPv6 prefixes are supported.

You must enter the *L4-src-port* and *L4-dst-port* arguments when the load-sharing mode is set to full, for example, when Layer 4 ports are included in the load-sharing hashing algorithm.

Examples

This example shows how to display the hardware IPv6-switching table entries:

```
Router# show mls cef ipv6

Codes:M-MPLS encap, + - Push label
Index Prefix Adjacency
524384 BEEF:6::6/128 punt
524386 5200::6/128 punt
524388 2929::6/128 punt
524390 6363::30/128 Fa1/48 , 0000.0001.0002
524392 3FFE:1B00:1:1:0:5EFE:1B00:1/128 punt
524394 2002:2929:6:2::6/128 punt
524396 2002:2929:6:1::6/128 punt
524398 6363::6/128 punt
524416 BEEF:6::/64 drop
524418 5200::/64 punt
524420 2929::/64 punt
524422 2002:2929:6:2::/64 punt
524424 2002:2929:6:1::/64 punt
524426 6363::/64 punt
524428 3FFE:1B00:1:1::/64 Tu4 , V6 auto-tunnel
524448 FEE0::/11 punt
524480 FE80::/10 punt
524512 FF00::/8 punt
524544 ::/0 drop
```

This example shows how to display the IPv6 entries for a specific IPv6 address and mask:

```
Router# show mls cef ipv6 2001:4747::/64

Codes:R - Recirculation, I-IP encap
M-MPLS encap, + - Push label
Index Prefix Out i/f Out Label
160 2001:4747::/64 punt
```

This example shows how to display all the IPv6-FIB entries that have per-prefix statistics available:

```
Router# show mls cef ipv6 accounting per-prefix

(I) BEEF:2::/64: 0 packets, 0 bytes

A - Active, I - Inactive
```

This example shows how to display detailed hardware information:

```
Router# show mls cef ipv6 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority
D - FIB Don't short-cut, m - mod-num
Format: IPv6_DA - (C | xtag vpn uvo prefix)
M(128 ): F | 1 FF 1 FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
```

```
V(128 ): C | 1 0 1 2001:4747::1253 (A:12 ,P:1,D:0,m:0 )
M(160 ): F | 1 FF 1 FFFF:FFFF:FFFF:FFFF::
V(160 ): C | 1 0 1 2001:4747:: (A:11 ,P:1,D:0,m:0 )
M(224 ): F | 1 FF 1 FFE0::
V(224 ): C | 1 0 1 FEE0:: (A:11 ,P:1,D:0,m:0 )
M(256 ): F | 1 FF 1 FFC0::
V(256 ): C | 1 0 1 FE80:: (A:12 ,P:1,D:0,m:0 )
M(352 ): F | 1 FF 1 FF00::
V(352 ): C | 1 0 1 FF00:: (A:12 ,P:1,D:0,m:0 )
M(480 ): F | 1 FF 1 ::
V(480 ): C | 1 0 1 :: (A:14 ,P:1,D:0,m:0
```

Related Commands

Command	Description
mls ipv6 acl compress address unicast	Turns on the compression of IPv6 addresses.
remote login	Accesses the Cisco 7600 series router console or a specific module.

show mls netflow ipv6

To display information about the hardware NetFlow IPv6 configuration, use the **show mls netflow ipv6** command in privileged EXEC mode.

show mls netflow ipv6 any

show mls netflow ipv6 count [**module** *number*]

show mls netflow ipv6 destination *ipv6-address*[*/ipv6-prefix*] [**count** [**module** *number*] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module** *number* | **nowrap** | **qos** | **source** *ipv6-address*[*/ipv6-prefix*] | **sw-installed** [**non-static** | **static**]]

show mls netflow ipv6 detail [**module** *number* | **nowrap** [**module** *number*]]

show mls netflow ipv6 dynamic [**count** [**module** *number*]] [**detail**] [**module** *number*] [**nowrap** [**module** *number*]] [**qos** [**module** *number*]] [**nowrap** [**module** *number*]]

show mls netflow ipv6 flow {**icmp** | **tcp** | **udp**} [**count** [**module** *number*] | **destination** *ipv6-address*[*/ipv6-prefix*] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module** *number* | **nowrap** | **qos** | **source** *ipv6-address*[*/ipv6-prefix*] | **sw-installed** [**non-static** | **static**]]

show mls netflow ipv6 [**module** *number*]

show mls netflow ipv6 qos [**module** *number* | **nowrap** [**module** *number*]]

show mls netflow ipv6 source *ipv6-address*[*/ipv6-prefix*] [**count** [**module** *number*] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module** *number* | **nowrap** | **qos** | **sw-installed** [**non-static** | **static**]]

Syntax Description

any	Displays the NetFlow-aging information.
count	Displays the total number of Multilayer Switching (MLS) NetFlow IPv6 entries.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
destination *ipv6-address*	Displays the entries for a specific destination IPv6 address.
/ipv6-prefix	(Optional) IPv6 prefix; valid values are from 0 to 128.
detail	Specifies a detailed output.
dynamic	Displays the hardware-created dynamic entries.
flow {**icmp** | **tcp** | **udp**}	Specifies the flow type.
nowrap	Turns off text wrapping.
qos	Displays information about quality of service (QoS) statistics.
source *ipv6-address*	(Optional) Displays the entries for a specific source IPv6 address.
sw-installed	(Optional) Displays the routing NetFlow entries.
non-static	(Optional) Displays information about the software-installed static IPv6 entries.
static	(Optional) Displays information about the software-installed nonstatic IPv6 entries.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed to add the **show mls netflow ipv6 qos** [**module** *number*] [**nowrap**] keywords and argument on the Supervisor Engine 720 only.
12.2(18)SXF	This command was changed as follows: • Removed support for the **any** keyword. • Added the */ipv6-prefix* argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display information about the hardware NetFlow configuration:

```
Router# show mls netflow ipv6

Displaying Netflow entries in Supervisor Earl
DstIP                                   SrcIP
-----------------------------------------------------------------------------
Prot:SrcPort:DstPort   Src i/f          :AdjPtr
Pkts        Bytes       Age  LastSeen   Attributes
-------------------------------------------------------------------------------------------
50::2                                   47::2
tcp :16     :32        Vl47             :0x0
23758       1425480     4    23:48:36   L3 (IPv6) - Dynamic
50::2                                   47::3
tcp :16     :32        Vl47             :0x0
23758       1425480     4    23:48:36   L3 (IPv6) - Dynamic
50::2                                   47::4
tcp :16     :32        Vl47             :0x0
23758       1425480     4    23:48:36   L3 (IPv6) - Dynamic
50::2                                   47::5
tcp :16     :32        Vl47             :0x0
23758       1425480     4    23:48:36   L3 (IPv6) - Dynamic
50::2                                   47::6
tcp :16     :32        Vl47             :0x0
23758       1425480     4    23:48:36   L3 (IPv6) - Dynamic
```

This example shows how to display IPv6 microflow policing information:

```
Router# show mls netflow ipv6 qos

Displaying Netflow entries in Supervisor Earl
DstIP                                   SrcIP
-----------------------------------------------------------------------------------
Prot:SrcPort:DstPort  Src i/f          :AdjPtr    Pkts         Bytes
-----------------------------------------------------------------------------------
LastSeen   QoS    PoliceCount  Threshold   Leak      Drop  Bucket
-------------------------------------------------------------------
101::3                                  100::2
icmp:0      :0        --               0x0          0            0
22:22:09   0x0    0                  0         0       NO  0
```

```
101::2                                  100::2
icmp:0      :0        --               0x0          0            0
22:22:09   0x0    0                  0         0       NO  0
```

This example shows how to display IPv6 microflow policing information for a specific module:

```
Router# show mls netflow ipv6 qos module 7

Displaying Netflow entries in module 7
DstIP                                   SrcIP
-------------------------------------------------------------------------------
Prot:SrcPort:DstPort  Src i/f          :AdjPtr    Pkts         Bytes
-------------------------------------------------------------------------------
LastSeen   QoS    PolicyCount  Threshold   Leak      Drop  Bucket
-------------------------------------------------------------------
101::2                                  100::2
icmp:0      :0        --               0x0          0            0
22:22:56   0x0    0                  0         0       NO  0
101::3                                  100::2
icmp:0      :0        --               0x0          0            0
22:22:56   0x0    0                  0         0       NO  0
```

This example shows the output display when you turn off text wrapping:

```
Router# show mls netflow ipv6 qos nowrap

Displaying Netflow entries in Supervisor Earl
DstIP                                   SrcIP
Prot:SrcPort:DstPort  Src i/f          :AdjPtr    Pkts         Bytes            LastSeen
QoS    PolicyCount  Threshold   Leak      Drop  Bucket
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
-----------------------------------------------
101::3                                  100::2                                  icmp:0
:0       --            0x0        0          0            22:22:19   0x0    0
0         0       NO  0
101::2                                  100::2                                  icmp:0
:0       --            0x0        0          0            22:22:19   0x0    0
0         0       NO  0
```

This example shows the output display when you turn off text wrapping for a specific module:

```
Router# show mls netflow ipv6 qos nowrap module 7

Displaying Netflow entries in module 7
DstIP                                   SrcIP
Prot:SrcPort:DstPort  Src i/f          :AdjPtr    Pkts         Bytes            LastSeen
QoS    PolicyCount  Threshold   Leak      Drop  Bucket
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
-----------------------------------------------
101::3                                  100::2                                  icmp:0
:0       --            0x0        0          0            22:22:38   0x0    0
0         0       NO  0
101::2                                  100::2                                  icmp:0
:0       --            0x0        0          0            22:22:38   0x0    0
0         0       NO  0
```

Related Commands

Command	Description
clear mls netflow	Clears the MLS NetFlow-shortcut entries.

show monitor event-trace cef ipv6

To display event trace messages for Cisco Express Forwarding IPv6 events, use the **show monitor event-trace cef ipv6** command in privileged EXEC mode.

show monitor event-trace cef ipv6 {*ipv6-address* {**all** [**detail**] | **back** {*minutes* | *hours*:*minutes*} [**detail**] | **clock** *hours*:*minutes* [*day month*] [**detail**] | **from-boot** *seconds* [**detail**] | **latest** [**detail**]} | **all** [**detail**] | **back** {*minutes* | *hours*:*minutes*} [**detail**] | **clock** *hours*:*minutes* [*day month*] [**detail**] | **from-boot** *seconds* [**detail**] | **latest** [**detail**] | **parameters**}

Syntax Description

ipv6-address	Specifies an IPv6 address. This address must be specified in hexadecimals using 16-bit values between colons, as specified in RFC 2373.
all	Displays all event trace messages currently in memory for Cisco Express Forwarding IPv6 events.
detail	(Optional) Displays detailed trace information for Cisco Express Forwarding IPv6 events.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
minutes	Time argument (mmm) in minutes.
hours:*minutes*	Time argument (hh:mm) in hours and minutes. You must enter the colon (:) in the argument.
clock	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
day month	(Optional) The day of the month from 1 to 31 and the name of the month of the year.
from-boot	Displays event trace messages starting after booting (uptime). To display the uptime, in seconds, enter the **show monitor event-trace cef from-boot ?** command.
seconds	(Optional) Displays event trace messages starting from a specified number of seconds after booting (uptime). Range: 0 to 3279.
latest	Displays only the event trace messages generated since the last **show monitor event-trace cef ipv6** command was entered.
parameters	Displays parameters configured for the trace.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show monitor event-trace cef ipv6** command to display trace message information for Cisco Express Forwarding IPv6 events.

The trace function is not locked while information is displayed to the console. This means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace cef ipv6** command generates a message indicating that some messages might be lost; however, messages continue to be displayed on the console. If the number of lost messages is excessive, the **show monitor event-trace cef ipv6** command stops displaying messages.

Examples

The following is a sample of the **show monitor event-trace cef ipv6 all** command:

```
Router# show monitor event-trace cef ipv6 all

*Aug 22 20:14:59.075:  [Default] *::*/*                Allocated FIB table
                      [OK]
*Aug 22 20:14:59.075:  [Default] *::*/*'00             Add source Default table
                      [OK]
*Aug 22 20:14:59.075:  [Default] ::/0'00               FIB add src DRH (ins)
                      [OK]
*Aug 22 20:14:59.075:  [Default] *::*/*'00             New FIB table
                      [OK]
```

Table 284 describes the significant fields shown in the display.

Table 284 show monitor event-trace cef ipv6 all Field Descriptions

Field	Description
*Aug 22 20:14:59.075:	Time stamp that indicates the month, day, and time when the event was captured.
[Default] *::*/*	Identifies the default VRF.
Allocated FIB table [OK]	Provides the event detail and indicates if the event happened. In this instance, a FIB table was allocated.

The following is sample output from the **show monitor event-trace cef ipv6 parameters** command:

```
Router# show monitor event-trace cef ipv6 parameters

Trace has 1000 entries
Stacktrace is disabled by default
Matching all events
```

Table 285 describes the significant fields shown in the display.

Table 285 show monitor event-trace cef ipv6 parameters Field Descriptions

Field	Description
Trace has 1000 entries	The size of the event logging buffer is 1000 entries.
Stacktrace is disabled by default	Stack trace at tracepoints is disabled.
Matching all events	Event tracing for all events is matched.

Related Commands

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

show monitor event-trace vpn-mapper

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

show mpls forwarding-table

To display the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB), use the **show mpls forwarding-table** command in user EXEC or privileged EXEC mode.

show mpls forwarding-table [*network* {*mask* | *length*} | **interface** *interface* | **labels** *label* [**-** *label*] | **lcatm atm** *atm-interface-number* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail slot** *slot-number*]

Syntax Description

network	(Optional) Destination network number.
mask	IP address of the destination mask whose entry is to be shown.
length	Number of bits in the mask of the destination.
interface *interface*	(Optional) Displays entries with the outgoing interface specified.
labels *label - label*	(Optional) Displays entries with the local labels specified.
lcatm atm *atm-interface-number*	Displays ATM entries with the specified Label Controlled Asynchronous Transfer Mode (LCATM).
next-hop *address*	(Optional) Displays only entries with the specified neighbor as the next hop.
lsp-tunnel	(Optional) Displays only entries with the specified label switched path (LSP) tunnel, or with all LSP tunnel entries.
tunnel-id	(Optional) Specifies the LSP tunnel for which to display entries.
vrf *vrf-name*	(Optional) Displays entries with the specified VPN routing and forwarding (VRF) instance.
detail	(Optional) Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit [MTU], and all labels).
slot *slot-number*	(Optional) Specifies the slot number, which is always 0.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T. The command was updated with MPLS terminology and command syntax.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. The command was modified to accommodate use of the MPLS experimental (EXP) level as a selection criterion for packet forwarding. The output display was modified to include a bundle adjacency field and exp (vcd) values when the optional **detail** keyword is specified.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. The IPv6 MPLS aggregate label and prefix information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S. The command output was modified to include explicit-null label information.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The output was changed in the following ways: • The term "tag" was replaced with the term "label." • The term "untagged" was replaced with the term "no label."
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. This command was modified to remove the **lsp-tunnel** keyword.
12.2(33)SXH	This command was modified. The command output shows the status of local labels in holddown for the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature. The status indicator showing that traffic is forwarded through an LSP tunnel is moved to the local label and the **lsp-tunnel** keyword was removed.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S. The output was modified to display the pseudowire identifier when the **interface** keyword is used.

Examples

The following is sample output from the **show mpls forwarding-table** command:

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
Label Label or VC   or Tunnel Id      switched  interface
26    No Label      10.253.0.0/16     0         Et4/0/0       10.27.32.4
28    1/33          10.15.0.0/16      0         AT0/0.1       point2point
29    Pop Label     10.91.0.0/16      0         Hs5/0         point2point
      1/36          10.91.0.0/16      0         AT0/0.1       point2point
30    32            10.250.0.97/32    0         Et4/0/2       10.92.0.7
      32            10.250.0.97/32    0         Hs5/0         point2point
34    26            10.77.0.0/24      0         Et4/0/2       10.92.0.7
      26            10.77.0.0/24      0         Hs5/0         point2point
35    No Label[T]   10.100.100.101/32 0         Tu301         point2point
36    Pop Label     10.1.0.0/16      0         Hs5/0         point2point
      1/37          10.1.0.0/16      0         AT0/0.1       point2point

[T]     Forwarding through a TSP tunnel.
        View additional labeling info with the 'detail' option
```

The following is sample output from the **show mpls forwarding-table** command when the IPv6 Provider Edge Router over MPLS feature is configured to allow IPv6 traffic to be transported across an IPv4 MPLS backbone. The labels are aggregated because there are several prefixes for one local label, and the prefix column contains "IPv6" instead of a target prefix.

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
Label Label or VC   or Tunnel Id      switched  interface
16    Aggregate     IPv6              0
17    Aggregate     IPv6              0
18    Aggregate     IPv6              0
19    Pop Label     192.168.99.64/30  0         Se0/0         point2point
```

```
20    Pop Label     192.168.99.70/32  0         Se0/0         point2point
21    Pop Label     192.168.99.200/32 0         Se0/0         point2point
22    Aggregate     IPv6              5424
23    Aggregate     IPv6              3576
24    Aggregate     IPv6              2600
```

The following is sample output from the **show mpls forwarding-table** command when you specify the **detail** keyword. If the MPLS EXP level is used as a selection criterion for packet forwarding, a bundle adjacency exp (vcd) field is included in the display. This field includes the EXP value and the corresponding virtual circuit descriptor (VCD) in parentheses. The line in the output that reads "No output feature configured" indicates that the MPLS egress NetFlow accounting feature is not enabled on the outgoing interface for this prefix.

```
Router# show mpls forwarding-table detail

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
label   label or VC     or Tunnel Id      switched  interface
16    Pop label       10.0.0.6/32        0         AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/12, MTU=4474, label Stack{}
      00010000AAAA030000008847
      No output feature configured
17    18            10.0.0.9/32        0         AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{18}
      00010000AAAA030000008847 00012000
      No output feature configured
18    19            10.0.0.10/32        0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{19}
      00010000AAAA030000008847 00013000
      No output feature configured
19    17            10.0.0.0/8         0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{17}
      00010000AAAA030000008847 00011000
      No output feature configured
20    20            10.0.0.0/8         0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{20}
      00010000AAAA030000008847 00014000
      No output feature configured
21    Pop label       10.0.0.0/24        0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/12, MTU=4474, label Stack{}
      00010000AAAA030000008847
      No output feature configured
22    Pop label       10.0.0.4/32         0        Et2/3         10.0.0.4
      MAC/Encaps=14/14, MTU=1504, label Stack{}
      000427AD10430005DDFE043B8847
      No output feature configured
```

The following is sample output from the **show mpls forwarding-table** command when you use the **detail** keyword. In this example, the MPLS egress NetFlow accounting feature is enabled on the first three prefixes, as indicated by the line in the output that reads "Feature Quick flag set."

```
Router# show mpls forwarding-table detail

Local  Outgoing    Prefix            Bytes label  Outgoing   Next Hop
label    label or VC   or Tunnel Id      switched   interface
16     Aggregate   10.0.0.0/8[V]     0
        MAC/Encaps=0/0, MTU=0, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
17     No label    10.0.0.0/8[V]      0          Et0/0/2    10.0.0.1
        MAC/Encaps=0/0, MTU=1500, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
18     No label    10.42.42.42/32[V] 4185       Et0/0/2    10.0.0.1
        MAC/Encaps=0/0, MTU=1500, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
19     2/33        10.41.41.41/32    0          AT1/0/0.1  point2point
        MAC/Encaps=4/8, MTU=4470, label Stack{2/33(vcd=2)}
        00028847 00002000
        No output feature configured
```

Cisco 10000 Series Examples

The following is sample output from the **show mpls forwarding-table** command for Cisco 10000 series routers:

```
Router# show mpls forwarding-table

Local   Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label   Label or VC   or Tunnel Id      Switched      interface
16      Pop Label     10.0.0.0/8        0             Fa1/0/0    10.0.0.2
        Pop Label     10.0.0.0/8        0             Fa1/1/0    10.0.0.2
17      Aggregate     10.0.0.0/8[V]     570           vpn2
21      Pop Label     10.11.11.11/32    0             Fa1/0/0    10.0.0.2
22      Pop Label     10.12.12.12/32    0             Fa1/1/0    10.0.0.2
23      No Label      10.3.0.0/16[V]     0             Fa4/1/0   10.0.0.2
```

The following is sample output from the **show mpls forwarding-table** command when you specify the **detail** keyword for Cisco 10000 series routers:

```
Router# show mpls forwarding-table detail

Local   Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label   Label or VC   or Tunnel Id      Switched      interface
16      Pop Label     10.0.0.0/8        0             Fa1/0/0    10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
        000B45C93889000B45C930218847
        No output feature configured
        Pop Label     10.0.0.0/8        0             Fa1/1/0     10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
        000B45C92881000B45C930288847
        No output feature configured
17      Aggregate    10.0.0.0/8[V]      570           vpn2
        MAC/Encaps=0/0, MRU=0, Label Stack{}
        VPN route: vpn2
        No output feature configured
21      Pop Label     10.11.11.11/32     0            Fa1/0/0     10.0.0.2
```

```
 MAC/Encaps=14/14, MRU=1500, Label Stack{}
000B45C93889000B45C930218847
No output feature configured
```

Table 286 describes the significant fields shown in the displays.

Table 286 show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this router.
Outgoing Label or VC **Note** This field is not supported on the Cisco 10000 series routers.	Label assigned by the next hop or the virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to next hop. The entries in this column are the following: • [T]—Forwarding is through an LSP tunnel. • No Label—There is no label for the destination from the next hop or label switching is not enabled on the outgoing interface. • Pop Label—The next hop advertised an implicit NULL label for the destination and the router removed the top label. • Aggregate—There are several prefixes for one local label. This entry is used when IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are sent. **Note** If IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network, “IPv6” is displayed here. • [V]—The corresponding prefix is in a VRF.
Bytes label switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.
Bundle adjacency exp(vcd)	Bundle adjacency information. Includes the MPLS EXP value and the corresponding VCD.
MAC/Encaps	Length in bytes of the Layer 2 header and length in bytes of the packet encapsulation, including the Layer 2 header and label header.
MTU	MTU of the labeled packet.
label Stack	All the outgoing labels. If the outgoing interface is transmission convergence (TC)-ATM, the VCD is also shown. **Note** TC-ATM is not supported on Cisco 10000 series routers.
00010000AAAA030000008847 00013000	The actual encapsulation in hexadecimal form. A space is shown between Layer 2 and the label header.

Explicit-Null Label Example

The following is sample output, including the explicit-null label = 0 (commented in bold), for the **show mpls forwarding-table** command on a CSC-PE router:

```
Router# show mpls forwarding-table

Local  Outgoing      Prefix            Bytes label  Outgoing   Next Hop
label  label or VC   or Tunnel Id      switched     interface
17     Pop label     10.10.0.0/32      0            Et2/0      10.10.0.1
18     Pop label     10.10.10.0/24     0            Et2/0      10.10.0.1
19     Aggregate     10.10.20.0/24[V]  0
20     Pop label     10.10.200.1/32[V] 0            Et2/1      10.10.10.1
21     Aggregate     10.10.1.1/32[V]   0
22     0             192.168.101.101/32[V]   \
                                       0            Et2/1      192.168.101.101
23     0             192.168.101.100/32[V]   \
                                       0            Et2/1      192.168.101.100
25     0             192.168.102.125/32[V] 0        Et2/1      192.168.102.125 !outlabel
value 0
```

Table 287 describes the significant fields shown in the display.

Table 287 show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this router.
Outgoing label or VC	Label assigned by the next hop or VPI/VCI used to get to the next hop. The entries in this column are the following: • [T]—Forwarding is through an LSP tunnel. • No label—There is no label for the destination from the next hop or that label switching is not enabled on the outgoing interface. • Pop label—The next hop advertised an implicit NULL label for the destination and that this router popped the top label. • Aggregate—There are several prefixes for one local label. This entry is used when IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network. • 0—The explicit null label value = 0.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are sent. **Note** If IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network, IPv6 is displayed here. • [V]—Means that the corresponding prefix is in a VRF.
Bytes label switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.

Cisco IOS Software Modularity: MPLS Layer 3 VPNs Example

The following is sample output from the **show mpls forwarding-table** command:

```
Router# show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  IPv4 VRF[V]      62951000      aggregate/v1
17    [H]  No Label   10.1.1.0/24      0             AT1/0/0.1 point2point
           No Label   10.1.1.0/24      0             PO3/1/0 point2point
      [T]  No Label   10.1.1.0/24      0             Tu1 point2point
18    [HT] Pop Label  10.0.0.3/32      0             Tu1 point2point
19    [H]  No Label   10.0.0.0/8       0             AT1/0/0.1 point2point
           No Label   10.0.0.0/8       0             PO3/1/0 point2point
20    [H]  No Label   10.0.0.0/8       0             AT1/0/0.1 point2point
           No Label   10.0.0.0/8       0             PO3/1/0 point2point
21    [H]  No Label   10.0.0.1/32      812           AT1/0/0.1 point2point
           No Label   10.0.0.1/32      0             PO3/1/0 point2point
22    [H]  No Label   10.1.14.0/24     0             AT1/0/0.1 point2point
           No Label   10.1.14.0/24     0             PO3/1/0 point2point
23    [HT] 16         172.1.1.0/24[V]  0             Tu1 point2point
24    [HT] 24         10.0.0.1/32[V]   0             Tu1 point2point
25    [H]  No Label   10.0.0.0/8[V]    0             AT1/1/0.1 point2point
26    [HT] 16         10.0.0.3/32[V]   0             Tu1 point2point
27         No Label   10.0.0.1/32[V]   0             AT1/1/0.1 point2point

[T]     Forwarding through a TSP tunnel.
        View additional labelling info with the 'detail' option
[H]     Local label is being held down temporarily.
```

Table 288 describes the Local Label fields relating to the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature.

Table 288 show mpls forwarding-table Field Descriptions

Field	Description
Local Label	Label assigned by this router. • [H]—Local labels are in holddown, which means that the application that requested the labels no longer needs them and stops advertising them to its labeling peers. The label's forwarding-table entry is deleted after a short, application-specific time. If any application starts advertising a held-down label to its labeling peers, the label could come out of holddown. **Note** [H] is not shown if labels are held down globally. A label enters global holddown after a stateful switchover or a restart of certain processes in a Cisco IOS modularity environment. • [T]—The label is forwarded through an LSP tunnel. **Note** Although [T] is still a property of the outgoing interface, it is shown in the Local Label column. • [HT]—Both conditions apply.

L2VPN Inter-AS Option B: Example

The following is sample output from the **show mpls forwarding-table interface** command. In this example, the pseudowire identifier (that is, 4096) is displayed in the Prefix or Tunel Id column. The **show mpls l2transport vc detail** command can be used to obtain more information about the specific pseudowire displayed.

```
Router# show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label    Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched       interface
1011       No Label   l2ckt(4096)          0          none       point2point
```

Table 289 describes the fields shown in the display.

Table 289 show mpls forwarding-table interface Field Descriptions

Field	Description
Local Label	Label assigned by this router.
Outgoing Label	Label assigned by the next hop or virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to the next hop.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are going.
Bytes Label Switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.

Table 289 show mpls forwarding-table interface Field Descriptions (continued)

Field	Description
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.

Related Commands

Command	Description
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.
show mpls l2transport vc detail	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a router.

show ntp associations

To display the status of Network Time Protocol (NTP) associations, use the **show ntp associations** command in user EXEC or privileged EXEC mode.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about each NTP association.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	Support for IPv6 was added.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

The following is sample output from the **show ntp associations** command:

```
Router> show ntp associations

     address         ref clock      st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 290 describes the significant fields shown in the display.

Table 290 show ntp associations Field Descriptions

Field	Description
address	Address of the peer.
ref clock	Address of the reference clock of the peer.
st	Stratum of the peer.
when	Time since the last NTP packet was received from the peer (in seconds).

Table 290 show ntp associations Field Descriptions (continued)

Field	Description
poll	Polling interval (in seconds).
reach	Peer reachability (bit string, in octal).
delay	Round-trip delay to the peer (in milliseconds).
offset	Relative time of the peer clock to the local clock (in milliseconds).
disp	Dispersion.
*	Synchronized to this peer.
#	Almost synchronized to this peer.
+	Peer selected for possible synchronization.
-	Peer is a candidate for selection.
~	Peer is statically configured.

The following is sample output from the **show ntp associations detail** command:

```
Router> show ntp associations detail

172.31.32.2 configured, insane, invalid, stratum 5
ref ID 172.31.32.1, time AFE252C1.6DBDDFF2 (00:12:01.428 PDT Mon Jul 5 1993)
our mode active, peer mode active, our poll intvl 1024, peer poll intvl 64
root delay 137.77 msec, root disp 142.75, reach 376, sync dist 215.363
delay 4.23 msec, offset -8.587 msec, dispersion 1.62
precision 2**19, version 3
org time AFE252E2.3AC0E887 (00:12:34.229 PDT Mon Jul 5 1993)
rcv time AFE252E2.3D7E464D (00:12:34.240 PDT Mon Jul 5 1993)
xmt time AFE25301.6F83E753 (00:13:05.435 PDT Mon Jul 5 1993)
filtdelay =     4.23    4.14    2.41    5.95    2.37    2.33    4.26    4.33
filtoffset =   -8.59   -8.82   -9.91   -8.42  -10.51  -10.77  -10.13  -10.11
filterror =     0.50    1.48    2.46    3.43    4.41    5.39    6.36    7.34

192.168.13.33 configured, selected, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE24F0E.14283000 (23:56:14.078 PDT Sun Jul 4 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 83.72 msec, root disp 217.77, reach 377, sync dist 264.633
delay 4.07 msec, offset 3.483 msec, dispersion 2.33
precision 2**6, version 3
org time AFE252B9.713E9000 (00:11:53.442 PDT Mon Jul 5 1993)
rcv time AFE252B9.7124E14A (00:11:53.441 PDT Mon Jul 5 1993)
xmt time AFE252B9.6F625195 (00:11:53.435 PDT Mon Jul 5 1993)
filtdelay =     6.47    4.07    3.94    3.86    7.31    7.20    9.52    8.71
filtoffset =    3.63    3.48    3.06    2.82    4.51    4.57    4.28    4.59
filterror =     0.00    1.95    3.91    4.88    5.84    6.82    7.80    8.77

192.168.13.57 configured, our_master, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE252DC.1F2B3000 (00:12:28.121 PDT Mon Jul 5 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 125.50 msec, root disp 115.80, reach 377, sync dist 186.157
delay 7.86 msec, offset 11.176 msec, dispersion 3.62
precision 2**6, version 2
org time AFE252DE.77C29000 (00:12:30.467 PDT Mon Jul 5 1993)
rcv time AFE252DE.7B2AE40B (00:12:30.481 PDT Mon Jul 5 1993)
xmt time AFE252DE.6E6D12E4 (00:12:30.431 PDT Mon Jul 5 1993)
filtdelay =    49.21    7.86    8.18    8.80    4.30    4.24    7.58    6.42
filtoffset =   11.30   11.18   11.13   11.28    8.91    9.09    9.27    9.57
```

```
filterror =     0.00    1.95    3.91    4.88    5.78    6.76    7.74    8.71
```

Table 291 describes the significant fields shown in the display.

Table 291 show ntp associations detail Field Descriptions

Field	Descriptions
configured	Peer was statically configured.
insane	Peer fails basic checks.
invalid	Peer time is believed to be invalid.
ref ID	Address of the machine the peer is synchronized to.
time	Last time stamp the peer received from its master.
our mode	Mode of the source relative to the peer (active/passive/client/server/bdcast/bdcast client).
peer mode	Peer's mode relative to the source.
our poll intvl	Source poll interval to the peer.
peer poll intvl	Peer's poll interval to the source.
root delay	Delay (in milliseconds) along the path to the root (ultimate stratum 1 time source).
root disp	Dispersion of the path to the root.
reach	Peer reachability (bit string in octal).
sync dist	Peer synchronization distance.
delay	Round-trip delay to the peer (in milliseconds).
offset	Offset of the peer clock relative to the system clock.
dispersion	Dispersion of the peer clock.
precision	Precision of the peer clock in Hertz.
version	NTP version number that the peer is using.
org time	Originate time stamp.
rcv time	Receive time stamp.
xmt time	Transmit time stamp.
filtdelay	Round-trip delay (in milliseconds) of each sample.
filtoffset	Clock offset (in milliseconds) of each sample.
filterror	Approximate error of each sample.
sane	Peer passes basic checks.
selected	Peer is selected for possible synchronization.
valid	Peer time is believed to be valid.
our_master	Local machine is synchronized to this peer.

Related Commands

Command	Description
show ntp status	Displays the status of the NTP.

show ntp status

To display the status of the Network Time Protocol (NTP), use the **show ntp status** command in user EXEC or privileged EXEC mode.

show ntp status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	Support for IPv6 was added.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

The following is sample output from the **show ntp status** command:

```
Router> show ntp status

Clock is synchronized, stratum 4, reference is 192.168.13.57
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is AFE2525E.70597B34 (00:10:22.438 PDT Mon Jul 5 1993)
clock offset is 7.33 msec, root delay is 133.36 msec
root dispersion is 126.28 msec, peer dispersion is 5.98 msec
```

Table 292 describes the significant fields shown in the display.

Table 292 show ntp status Field Descriptions

Field	Description
synchronized	System is synchronized to an NTP peer.
stratum	NTP stratum of this system.
reference	Address of the peer the system is synchronized to.
nominal freq	Nominal frequency of the system hardware clock (in Hertz).
actual freq	Measured frequency of the system hardware clock (in Hertz).
precision	Precision of the clock of this system (in Hertz).

Table 292 show ntp status Field Descriptions (continued)

Field	Description
reference time	Reference time stamp.
clock offset	Offset of the system clock to the synchronized peer (in milliseconds).
root delay	Total delay along the path to the root clock (in milliseconds).
root dispersion	Dispersion of the root path.
peer dispersion	Dispersion of the synchronized peer.

Related Commands

Command	Description
show ntp associations	Displays the status of the NTP associations.

show ospfv3 border-routers

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

show ospfv3 [*process-id*] [*address-family*] **border-routers**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

show ospfv3 database

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

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

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area. The *area-id* argument can only be used if the *process-id* argument is specified.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
database-summary	(Optional) Displays how many of each type of LSAs exist for each area in the database, and the total.
internal	(Optional) Internal LSA information.
external	(Optional) Displays information only about the external LSAs.
ipv6-prefix	(Optional) Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
grace	(Optional) Displays information about OSPFv3 graceful restart.
link-state-id	(Optional) An integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
inter-area prefix	(Optional) Displays information only about LSAs based on inter-area prefix LSAs.
inter-area router	(Optional) Displays information only about LSAs based on inter-area router LSAs.
destination-router-id	(Optional) The specified destination router ID.
link	(Optional) Displays information about the link LSAs.
interface	(Optional) Displays information about the LSAs filtered by interface context.
interface-name	(Optional) Specifies the LSA interface.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.
prefix	(Optional) Displays information on the intra-area-prefix LSAs.

promiscuous	(Optional) Displays temporary LSAs in a Mobile Ad Hoc Network (MANET).
ref-lsa {**router** | **network**}	(Optional) Further filters the prefix LSA type.
router	(Optional) Displays information only about the router LSAs.
unknown	(Optional) Displays all LSAs with unknown types.
area	(Optional) Filters unknown area LSAs.
as	(Optional) Filters unknown autonomous system (AS) LSAs.
link	(Optional) When following the **unknown** keyword, the **link** keyword filters link-scope LSAs.
adv-router *router-id*	(Optional) Displays all the LSAs of the advertising router. This argument must be in the form documented in RFC 2740 where the address is specified in hexadecimal using 16-bit values between colons.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ospfv3 database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
```

```
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

Table 293 describes the significant fields shown in the display.

Table 293 show ospfv3 database Field Descriptions

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

show ospfv3 events

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

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

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
generic	(Optional) Generic information regarding OSPFv3 events.
interface	(Optional) Interface state change events, including old and new states.
lsa	(Optional) LSA arrival and LSA generation events.
neighbor	(Optional) Neighbor state change events, including old and new states.
reverse	(Optional) Keyword to allow the display of events in reverse–from the latest to the oldest or from oldest to the latest.
rib	(Optional) Routing Information Base (RIB) update, delete, and redistribution events.
spf	(Optional) Scheduling and SPF run events.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ospfv3 events
```

show ospfv3 flood-list

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

show ospfv3 [*process-id*] [*area-id*] [*address-family*] **flood-list** *interface-type interface-number*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
interface-type	Interface type over which the LSAs will be flooded.
interface-number	Interface number over which the LSAs will be flooded.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use this command to display OSPFv3 packet pacing.

Examples

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

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

show ospfv3 graceful-restart

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

show ospfv3 [*process-id*] [*address-family*] **graceful-restart**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

The following example displays OSPFv3 graceful restart information :

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

show ospfv3 interface

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

show ospfv3 [*process-id*] [*area-id*] [*address-family*] **interface** [*type number*] [**brief**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information about a specified area only.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
type number	(Optional) Interface type and number.
brief	(Optional) Displays brief overview information for OSPFv3 interfaces, states, addresses and masks, and areas on the router.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# show ospfv3 interface

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

```
 Relaying enabled
Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
Router#
```

Table 294 describes the significant fields shown in the display.

Table 294 show ospfv3 interface Field Descriptions

Field	Description
Ethernet0/0	Status of the physical link and the operational status of the protocol.
Link Local Address	Interface IPv6 address.
Area 0, Process ID 100, Instance ID 0, Router ID 172.16.3.3	Area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type MANET, Cost: 10 (dynamic), Cost hysteresis: Disabled	Network type and link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Timer intervals configured	Configuration of timer intervals, including hello-increment and dead-interval.
Hello due in 00:00:01	Number of seconds until the next hello packet is sent from this interface.
Supports Link-local Signaling (LLS)	Indicates that LLS is supported.
Last flood scan length is 2, maximum is 2	Indicates length of last flood scan and the maximum length.
Last flood scan time is 0 msec, maximum is 0 msec	Indicates how many milliseconds the last flood scan occurred and the maximum time length.
Neighbor Count	Count of network neighbors and a list of adjacent neighbors.
Adjacent with neighbor 2.2.2.2	Lists the adjacent neighbor.
Suppress hello for 0 neighbor(s)	Indicates the number of neighbors to suppress hello messages

show ospfv3 neighbor

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

show ospfv3 [*process-id*] [*area-id*] [*address-family*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
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
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Examples

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

```
Router# show ospfv3 neighbor

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

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

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

```
Router# show ospfv3 neighbor detail
Neighbor 42.4.4.4, interface address 4.4.4.4
     In the process ID 42 area 0 via interface vmi1
Neighbor: interface-id 12, link-local address FE80::A8BB:CCFF:FE01:5800
    Neighbor priority is 1, State is FULL, 6 state changes
```

```
     Options is 0x000F12 in Hello (E-Bit, R-bit, AF-Bit, L-Bit, I-Bit, F-Bit)
     Options is 0x000112 in DBD (E-Bit, R-bit, AF-Bit)
     Dead timer due in 00:00:33
     Neighbor is up for 00:09:43
     Index 1/1/1, retransmission queue length 0, number of retransmission 0
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 0, maximum is 0
     Last retransmission scan time is 0 msec, maximum is 0 msec
     Neighbor is incremental Hello capable
     Last known SCS number 1
     Neighbor's willingness 128
     We are standby relay for the neighbor
     This neighbor is standby relay for us
     Neighbor is running Manet Version 10
Neighbor 4.4.4.4
      In the process ID 100 area 0 via interface vmi1
Neighbor: interface-id 12, link-local address FE80::A8BB:CCFF:FE01:5800
     Neighbor priority is 1, State is FULL, 6 state changes
     Options is 0x000E13 in Hello (V6-Bit, E-Bit, R-bit, L-Bit, I-Bit, F-Bit)
     Options is 0x000013 in DBD (V6-Bit, E-Bit, R-bit)
     Dead timer due in 00:00:37
     Neighbor is up for 00:09:43
     Index 1/1/1, retransmission queue length 0, number of retransmission 0
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 0, maximum is 0
     Last retransmission scan time is 0 msec, maximum is 0 msec
     Neighbor is incremental Hello capable
     Last known SCS number 1
     Neighbor's willingness 128
Two-hop neighbors:
     5.5.5.5
     We are standby relay for the neighbor
     This neighbor is active relay for us
     Neighbor is running Manet Version 10
     Selective Peering is enabled
     1 paths to this neighbor
Neighbor peering state: Slave, local peering state: Master,
     Default cost metric is 0
     Minimum incremental cost is 10
```

Table 295 describes the significant fields shown in the display.

Table 295 show ospfv3 neighbor Field Descriptions

Field	Description
Neighbor ID; Neighbor	Neighbor router ID.
In the area	Area and interface through which the OSPFv3 neighbor is known.
Pri; Neighbor priority	Router priority of the neighbor, neighbor state.
State	OSPFv3 state.
State changes	Number of state changes since the neighbor was created.
Options	Hello packet options field contents (E-bit only). Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)
Dead timer due in	Expected time before Cisco IOS software declares the neighbor dead.

Table 295 show ospfv3 neighbor Field Descriptions (continued)

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

Table 295 show ospfv3 neighbor Field Descriptions (continued)

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

show ospfv3 request-list

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

show ospfv3 [*process-id*] [*area-id*] [*address-family*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
neighbor	(Optional) Displays the list of all LSAs requested by the router from this neighbor.
interface	(Optional) Displays the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Displays the list of all LSAs requested by the router on this interface, from this neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ospfv3 request-list

            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)

 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
```

```
1       0.0.0.0         192.168.255.2   0x800000C8  0       0x000BCA
1       0.0.0.0         192.168.255.1   0x800000C5  1       0x008CD1
2       0.0.0.3         192.168.255.3   0x800000A9  774     0x0058C0
2       0.0.0.2         192.168.255.3   0x800000B7  1       0x003A63
```

Table 296 describes the significant fields shown in the display.

Table 296 show ospfv3 request-list Field Descriptions

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

show ospfv3 retransmission-list

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

show ospfv3 [*process-id*] [*area-id*] [*address-family*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.
interface	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.
interface-neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ospfv3 retransmission-list

        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)

 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

Table 297 describes the significant fields shown in the display.

Table 297 show ospfv3 retransmission-list Field Descriptions

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

show ospfv3 statistic

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

show ospfv3 [*process-id*] [*address-family*] **statistic** [**detail**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
detail	(Optional) Displays statistics separately for each OSPFv3 area and includes additional, more detailed statistics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

The following example provides detailed statistics for each OSPFv3 area:

```
Router# show ospfv3 statistics detail

  Area 0: SPF algorithm executed 3 times

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

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

Table 267 describes the significant fields shown in the display.

Table 298 show ospfv3 statistics Field Descriptions

Field	Description
Area	OSPF area ID.
SPF	Number of SPF algorithms executed in the OSPF area. The number increases by one for each SPF algorithm that is executed in the area.
Executed ago	Time in milliseconds that has passed between the start of the SPF algorithm execution and the current time.
SPF type	SPF type can be Full or Incremental.
SPT	Time in milliseconds required to compute the first stage of the SPF algorithm (to build a short path tree). The SPT time plus the time required to process links to stub networks equals the Intra time.
Ext	Time in milliseconds for the SPF algorithm to process external and not so stubby area (NSSA) LSAs and to install external and NSSA routes in the routing table.
Total	Total duration time in milliseconds for the SPF algorithm process.
LSIDs processed	Number of LSAs processed during the SPF calculation: • N—Network LSA. • R—Router LSA. • SA—Summary Autonomous System Boundary Router (ASBR) (SA) LSA. • SN—Summary Network (SN) LSA. • Stub—Stub links. • X7—External Type-7 (X7) LSA.

show ospfv3 summary-prefix

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

show ospfv3 [*process-id*] [*address-family*] **summary-prefix**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ospfv3 summary-prefix

OSPFv3 Process 1, Summary-prefix

FEC0::/24 Metric 16777215, Type 0, Tag 0
```

Table 299 describes the significant fields shown in the display.

Table 299 show ospfv3 summary-prefix Field Descriptions

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

show ospfv3 timers rate-limit

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

show ospfv3 [*process-id*] [*address-family*] **timers rate-limit**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ospfv3 timers rate-limit

List of LSAs that are in rate limit Queue

    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
```

Table 300 describes the significant fields shown in the display.

Table 300 show ospfv3 timers rate-limit Field Descriptions

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

show ospfv3 traffic

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

show ospfv3 [*process-id*] [*address-family*] **traffic** [*interface-type interface-number*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
interface-type interface-number	(Optional) Type and number associated with a specific OSPFv3 interface.

Command Default

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ospfv3 traffic

OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored

  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
```

```
        OSPFv3 Router with ID (10.1.1.4) (Process ID 6)

OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2


Interface statistics:


    Interface Serial2/0

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      5                    196
  RX DB des     4                    172
  RX LS req     1                    52
  RX LS upd     4                    320
  RX LS ack     2                    112
  RX Total      16                   852

  TX Failed     0                    0
  TX Hello      8                    304
  TX DB des     3                    144
  TX LS req     1                    52
  TX LS upd     3                    252
  TX LS ack     3                    148
  TX Total      18                   900

OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,


    Interface Ethernet0/0

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      6                    240
  RX DB des     3                    144
  RX LS req     1                    52
  RX LS upd     5                    372
  RX LS ack     2                    152
  RX Total      17                   960

  TX Failed     0                    0
  TX Hello      11                   420
  TX DB des     9                    312
  TX LS req     1                    52
  TX LS upd     5                    376
  TX LS ack     3                    148
  TX Total      29                   1308
```

```
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,


Summary traffic statistics for process ID 6:

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      11                   436
  RX DB des     7                    316
  RX LS req     2                    104
  RX LS upd     9                    692
  RX LS ack     4                    264
  RX Total      33                   1812

  TX Failed     0                    0
  TX Hello      19                   724
  TX DB des     12                   456
  TX LS req     2                    104
  TX LS upd     8                    628
  TX LS ack     6                    296
  TX Total      47                   2208

OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

Table 301 describes the significant fields shown in the display.

Table 301 show ospfv3 traffic Field Descriptions

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

Table 301 show ospfv3 traffic Field Descriptions (continued)

Field	Description
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 OSPFv3 link-state advertisement (LSA). The discarded packet is counted under the appropriate discard reason.
Summary traffic statistics for process ID	Summary traffic statistics accumulated for an OSPFv3 process. **Note** The OSPFv3 process ID is a unique value assigned to the OSPFv3 process in the configuration. The value for the received errors is the sum of the OSPFv3 header errors that are detected by the OSPFv3 process, unlike the sum of the checksum errors that are listed in the global OSPFv3 statistics.

show ospfv3 virtual-links

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

show ospfv3 [*process-id*] [*address-family*] **virtual-links**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ospfv3 virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

Table 302 describes the significant fields shown in the display.

Table 302 show ospfv3 virtual-links Field Descriptions

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

The following sample output from the **show ospfv3 virtual-links** command has two virtual links. One is protected by authentication, and the other is protected by encryption.

```
Router# show ospfv3 virtual-links

Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
   Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial12/0, Cost of using 64
   NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/2/4, retransmission queue length 0, number of retransmission 1
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
   Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial11/0, Cost of using 128
   MD5 authentication SPI 940, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/1/3, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
```

show platform software ipv6-multicast

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# show platform software ipv6-multicast capability

 Hardware switching for ipv6 is Enabled
 (S,G) forwarding for ipv6 supported using Netflow
 (*,G) bridging for ipv6 is supported using Fib
 Directly-connected entries for IPv6 is supported using ACL-TCAM.

Current System HW Replication Mode : Egress
Audo-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
   2 Egress                 Egress
   5 Egress                 Egress
```

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

```
Router# show platform software ipv6-multicast connected

IPv6 Multicast Subnet entries
Flags : H - Installed in ACL-TCAM
        X - Not installed in ACL-TCAM due to
            label-full exception

Interface: Vlan40 [ H ]
         S:40::1 G:FF00::
         S:0:5000::2 G:FF00::
         S:5000::2 G:FF00::
Interface: Vlan30 [ H ]
         S:30::1 G:FF00::
Interface: Vlan20 [ H ]
         S:20::1 G:FF00::
Interface: Vlan10 [ H ]
         S:10::1 G:FF00::
```

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

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

---- SLOT [7] ----

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

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

```
Router# show platform software ipv6-multicast statistics

IPv6 Multicast HW-switching Status                 : Enabled
IPv6 Multicast (*,G) HW-switching Status           : Disabled
IPv6 Multicast Subnet-entries Status               : Enabled
Default MFIB IPv6-table                            : 0x5108F770
(S,G,C) flowmask index                             : 3
(*,G,C) flowmask index                             : 65535

General Counters
--------------------------------------------------+------+
Mfib-hw-entries count                              0
Mfib-add count                                     4
Mfib-modify count                                  2
Mfib-delete count                                  2
Mfib-NP-entries count                              0
Mfib-D-entries count                               0
Mfib-IC-entries count                              0
Error Counters
--------------------------------------------------+------+
ACL flowmask err count                             0
ACL TCAM exptn count                               0
ACL renable count                                  0
Idb Null error                                     0
```

This example shows how to display the IPv6-multicast hardware shortcut count:

```
Router# show platform software ipv6-multicast summary

IPv6 Multicast Netflow SC summary on Slot[7]:
Shortcut Type               Shortcut count
---------------------------+--------------
(S, G)                      0

IPv6 Multicast FIB SC summary on Slot[7]:
Shortcut Type               Shortcut count
---------------------------+--------------
(*, G/128)                  0
(*, G/m)                    0
```

Related Commands

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

show platform software vpn

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB1	This command was introduced on the Cisco 7600 series routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

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

Examples

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

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

show route-map

To display static and dynamic route maps, use the **show route-map** command in privileged EXEC mode.

show route-map [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**] [**detailed**]

Syntax Description

map-name	(Optional) Name of a specific route map.
dynamic	(Optional) Displays dynamic route map information.
dynamic-map-name	(Optional) Name of a specific dynamic route map.
application	(Optional) Displays dynamic route maps based on applications.
application-name	(Optional) Name of a specific application.
all	(Optional) Displays all static and dynamic route maps.
detailed	(Optional) Displays the details of the access control lists (ACLs) that have been used in the **match** clauses for dynamic route maps.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and support for continue clauses was integrated into the command output.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBA	The output was enhanced to display dynamically assigned route maps to VRF tables.
12.2(15)T	An additional counter collect policy routing statistic was integrated into Cisco IOS Release 12.2(15)T.
12.3(2)T	Support for continue clauses was integrated into Cisco IOS Release 12.3(2)T.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.3(7)T	The **dynamic**, **application**, and **all** keywords were added.
12.0(28)S	The support for recursive **next-hop** clause was added.
12.3(14)T	The support for recursive **next-hop** clause was integrated into Cisco IOS Release 12.3(14)T. Support for the map display extension functionality was added. The **detailed** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Cisco IOS XE Release 2.2	In Cisco IOS XE Release 2.2 this command was introduced on the Cisco ASR 1000 Series Routers.
15.0(1)M	This command was modified. The **detailed** keyword was removed.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

You can view static and dynamic route maps with the **show route-map** command. For Cisco IOS Release 12.3(14)T and later 12.4 and 12.4T releases, you can display the ACL-specific information that pertains to the route map in the same display without having to execute a **show route-map** command to display each ACL that is associated with the route map.

Redistribution

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

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

Use **route maps** when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the router global configuration command. The source routing protocol is the one you specify with the **redistribute** router configuration command. See the "Examples" section for an illustration of how route maps are configured.

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

Examples

The **show route-map** command will display configured route-maps, match, set, and continue clauses. The output will vary depending on which keywords are included with the command, and which software image is running in your router, as shown in the following examples:

- show route-map Command with No Keywords Specified: Example, page 2132
- show route-map Command with Dynamic Route Map Specified: Example, page 2134
- show route-map Command with Detailed ACL Information for Route Maps Specified: Example, page 2135
- show route-map Command with VRF Autoclassification: Example, page 2135

show route-map Command with No Keywords Specified: Example

The following is sample output from the **show route-map** command:

```
Router# show route-map

route-map ROUTE-MAP-NAME, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    metric 10
  Continue: sequence 40
  Set clauses:
    as-path prepend 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 20
```

```
  Match clauses:
    ip address (access-lists): 2
    metric 20
  Set clauses:
    as-path prepend 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 30
  Match clauses:
  Continue: to next entry 40
  Set clauses:
    as-path prepend 10 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, deny, sequence 40
  Match clauses:
    community (community-list filter): 20:2
  Set clauses:
    local-preference 100
  Policy routing matches: 0 packets, 0 bytes
route-map LOCAL-POLICY-MAP, permit, sequence 10
  Match clauses:
  Set clauses:
    community 655370
  Policy routing matches: 0 packets, 0 bytes
```

The following example shows Multiprotocol Label Switching (MPLS)-related route map information:

```
Router# show route-map

route-map OUT, permit, sequence 10
Match clauses:
  ip address (access-lists): 1
Set clauses:
  mpls label
Policy routing matches: 0 packets, 0 bytes

route-map IN, permit, sequence 10
Match clauses:
  ip address (access-lists): 2
  mpls label
Set clauses:
Policy routing matches: 0 packets, 0 bytes
```

Table 301 describes the significant fields shown in the display.

Table 303 show route-map Field Descriptions

Field	Description
route-map ROUTE-MAP-NAME	Name of the route map.
permit	Indicates that the route is redistributed as controlled by the set actions.
sequence	Number that indicates the position a new route map is to have in the list of route maps already configured with the same name.
Match clauses: tag	Match criteria—Conditions under which redistribution is allowed for the current route map.
Continue:	Continue clause—Shows the configuration of a continue clause and the route-map entry sequence number that the continue clause will go to.

Table 303 show route-map Field Descriptions (continued)

Field	Description
Set clauses: metric	Set actions—The particular redistribution actions to perform if the criteria enforced by the **match** commands are met.
Policy routing matches:	Number of packets and bytes that have been filtered by policy routing.

show route-map Command with Dynamic Route Map Specified: Example

The following is sample output from the **show route-map** command when entered with the **dynamic** keyword:

```
Router# show route-map dynamic

route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 0, identifier 1137954548
  Match clauses:
    ip address (access-lists): PBR#1 PBR#2
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 1, identifier 1137956424
  Match clauses:
    ip address (access-lists): PBR#3 PBR#4
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:01:26.619-1-AppSpec, permit, sequence 2, identifier 1124436704
  Match clauses:
    ip address (access-lists): PBR#5 PBR#6
    length 10 100
  Set clauses:
    ip next-hop 172.16.1.1
    ip gateway 172.16.1.1
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

The following is sample output from the **show route-map** command when entered with the **dynamic** and **application** keywords:

```
Router# show route-map dynamic application

Application - AAA
  Number of active routemaps = 1
```

When you specify an application name, only dynamic routes for that application are shown. The following is sample output from the **show route-map** command when entered with the **dynamic** and **application** keywords and the AAA application name:

```
Router# show route-map dynamic application AAA

AAA
  Number of active rmaps = 2
AAA-02/06/04-14:01:26.619-1-AppSpec
AAA-02/06/04-14:34:09.735-2-AppSpec

Router# show route-map dynamic AAA-02/06/04-14:34:09.735-2-AppSpec

route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 0, identifier 1128046100
  Match clauses:
    ip address (access-lists): PBR#7 PBR#8
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
```

```
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 1, identifier 1141277624
  Match clauses:
    ip address (access-lists): PBR#9 PBR#10
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-02/06/04-14:34:09.735-2-AppSpec, permit, sequence 2, identifier 1141279420
  Match clauses:
    ip address (access-lists): PBR#11 PBR#12
    length 10 100
  Set clauses:
    ip next-hop 172.16.1.12
    ip gateway 172.16.1.12
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 2
```

show route-map Command with Detailed ACL Information for Route Maps Specified: Example

The following is sample output from the **show route-map** command with the **dynamic** and **detailed** keywords entered:

```
Router# show route-map dynamic detailed

route-map AAA-01/20/04-22:03:10.799-1-AppSpec, permit, sequence 1, identifier 29675368
Match clauses:
ip address (access-lists):
Extended IP access list PBR#3
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input fragments
Extended IP access list PBR#4
1 permit icmp 0.0.16.12 1.204.167.240 10.1.1.0 0.0.0.255 syn dscp af12 log-input fragments
Set clauses:
ip next-hop 172.16.1.14
ip gateway 172.16.1.14
Policy routing matches: 0 packets, 0 bytes
```

show route-map Command with VRF Autoclassification: Example

The following is sample output from the **show route-map** command when a specified VRF is configured for VRF autoclassification:

```
Router# show route-map dynamic

route-map None-06/01/04-21:14:21.407-1-IP VRF, permit, sequence 0
identifier 1675771000
 Match clauses:
 Set clauses: vrf red
 Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match tag	Redistributes routes in the routing table that match the specified tags.

show sccp

To display Skinny Client Control Protocol (SCCP) information such as administrative and operational status, use the **show sccp** command in user EXEC or privileged EXEC mode.

show sccp [**all** | **ccm group** [*number*] | **connections** [**details** | **internal** | **rsvp** | **summary**] | **server** | **statistics** | **call-identifications** | **call-references**]

Syntax Description

all	(Optional) Specifies all Skinny Client Control Protocol (SCCP) global information.
ccm	(Optional) Displays SCCP Cisco Unified Communications Manager (CUCM) group related information.
group	(Optional) Displays CUCM groups.
number	(Optional) CUCM group number that needs to be displayed.
connections	(Optional) Specifies information about the connections controlled by the SCCP transcoding and conferencing applications.
details	(Optional) Displays SCCP connections in detail.
internal	(Optional) Displays information about SCCP internal connections.
rsvp	(Optional) Displays Resource Reservation Protocol (RSVP) information about SCCP connections.
summary	(Optional) Displays information about SCCP connections.
server	(Optional) Displays SCCP server information.
statistics	(Optional) Specifies statistical information for SCCP transcoding and conferencing applications.
call-identifications	(Optional) Displays the following identification numbers that is associated with each leg of a call: • Session • Call Reference • Connection • Call • Bridge • Profile
call-references	(Optional) Displays codec, port, ID numbers for each leg of a call.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(6)T	This command was modified. The **rsvp** keyword was added.

Release	Modification
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.
12.3(8)T	This command was modified. The following keywords and arguments were added: **ccm**, **connections**, **details**, **group**, **internal,** *number,* **summary**.
12.4(11)XW1	This command was modified. The stype field was added to the show output to show whether a connections is encrypted.
12.4(15)XY	This command was modified. The **statistics** and **server** keywords were added.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information and it was integrated into Cisco IOS Release 12.2(13)T.
15.1(4)M	This command was modified. The **call-identifications** and **call-references** keywords were added.

Usage Guidelines

The router on which you use the **show sccp** command must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital signal processor (DSP) resources.

Use the **show sccp ccm** group command to show detailed information about all groups assigned to the Cisco Unified CallManager. The optional group-number argument can be added to select details about a specific group.

Configure the **show sccp server statistics** command on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller where no SCCP phone is registered, to show the statistical counts on the SCCP server. The counts display queuing errors and message drops on the transcoder alone when it is on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller.

When the **show sccp server statistics** command is used on the Cisco Unified Manager Express (CME), it is recommended for use together with the clear sccp server statistics command.

Examples

In the following sample output, the gateway IP address can be an IPv4 or IPv6 address when it operates on an IPv4/IPv6 dual stack.

```
Router# show sccp
SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/0
        IPv6 Address: 2001:DB8:C18:1::3
        IPv4 Address: 10.4.34.100
        Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 172.19.242.27, Port Number: 2000
                Priority: N/A, Version: 5.0.1, Identifier: 4
                Trustpoint: N/A
Call Manager: 2001:DB8:C18:1::100, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 1
                Trustpoint: N/A
```

Table 304 describes the significant fields shown in the display.

Table 304 show sccp Field Descriptions

Field	Description
SCCP Admin State	Current state of the SCCP session.
Gateway Local Interface	Local interface that SCCP applications use to register with Cisco Unified Communications Manager.
IP precedence	Sets the IP precedence value for SCCP.
User Masked Codec list	Codec to mask.
Call Manager	Cisco Unified CallManager server information.

The following is sample output from this command for IPv4 only. The field descriptions are self-explanatory.

```
Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 10.10.10.11, Port Number: 0
Switchover Method: IMMEDIATE, Switchback Method: GUARD_TIMER
Switchback Guard Timer: 1200 sec, IP Precedence: 5
Max Supported MTP sessions: 100
Transcoding Oper State: ACTIVE - Cause Code: NONE
Active CallManager: 10.10.10.35, Port Number: 2000
TCP Link Status: CONNECTED
Conferencing Oper State: DOWN - Cause Code: DSPFARM_DOWN
Active CallManager: NONE
TCP Link Status: NOT_CONNECTED
CallManager: 10.10.10.37, Port Number: 2000
Priority: 3, Version: 3.1
CallManager: 10.10.10.35, Port Number: 2000
Priority: 2, Version: 3.0
```

The following sample shows statistical information for SCCP transcoding and conferencing applications.

```
Router# show sccp statistics

SCCP Transcoding Application Statistics:
TCP packets rx 548, tx 559
Unsupported pkts rx 3, Unrecognized pkts rx 0
Register tx 3, successful 3, rejected 0, failed 0
KeepAlive tx 543, successful 540, failed 2
OpenReceiveChannel rx 2, successful 2, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 2, successful 2, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 1, Switchback 1

SCCP Conferencing Application Statistics:
TCP packets rx 0, tx 0
Unsupported pkts rx 0, Unrecognized pkts rx 0
Register tx 0, successful 0, rejected 0, failed 0
KeepAlive tx 0, successful 0, failed 0
OpenReceiveChannel rx 0, successful 0, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 0, successful 0, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
```

```
MediaStreamingFailure rx 0
Switchover 0, Switchback 0
```

In the following example, the secure value of the stype field indicates that the conection is encrypted. The field descriptions are self-explanatory.

```
Router# show sccp connections

sess_id    conn_id    stype        mode codec   ripaddr       rport sport

16777222   16777409   secure-xcode sendrecv g729b   10.3.56.120   16772 19534
16777222   16777393   secure-xcode sendrecv g711u   10.3.56.50    17030 18464

Total number of active session(s) 1, and connection(s) 2
```

The following example shows the remote IP addresses of active RTP sessions, each of which shows either an IPv4 or an IPv6 address.

```
Router# show sccp connections

sess_id  conn_id  stype  mode    codec sport rport ripaddr

16777219 16777245 conf  sendrecv g711u 16516 27814 10.3.43.46
16777219 16777242 conf  sendrecv g711u 17712 18028 10.3.43.2
16777219 16777232 conf  sendrecv g711u 16890 19440 10.3.43.2
16777219 16777228 conf  sendrecv g711u 19452 17464 10.3.43.2
16777220 16777229 xcode sendrecv g711u 17464 19452 10.3.43.2
16777220 16777227 xcode sendrecv g729b 19466 19434 2001:0DB8:C18:1:212:79FF:FED7:B254
16777221 16777233 mtp   sendrecv g711u 19440 16890 10.3.43.2
16777221 16777231 mtp   sendrecv g711u 17698 17426 2001:0DB8:C18:1:212:79FF:FED7:B254
16777223 16777243 mtp   sendrecv g711u 18028 17712 10.3.43.2
16777223 16777241 mtp   sendrecv g711u 16588 19446 2001:0DB8:C18:1:212:79FF:FED7:B254
```

The following is sample output for the two Cisco CallManager Groups assigned to the Cisco Unified CallManager: group 5 named "boston office" and group 988 named "atlanta office".

```
Router# show sccp ccm group

CCM Group Identifier: 5
 Description: boston office
 Binded Interface: NONE, IP Address: NONE
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 3, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 1200 sec
 Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
 Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
 Signaling DSCP value: default, Audio DSCP value: default

CCM Group Identifier: 988
 Description: atlanta office
 Binded Interface: NONE, IP Address: NONE
 Associated CCM Id: 1, Priority in this CCM Group: 1
 Associated Profile: 6, Registration Name: MTP123456789988
 Associated Profile: 10, Registration Name: CFB123456789966
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 5, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 10 sec
 Switchover Method: IMMEDIATE, Switchback Method: IMMEDIATE
 Switchback Interval: 15 sec, Switchback Timeout: 0 sec
 Signaling DSCP value: default, Audio DSCP value: default
```

Table 305 describes the significant fields shown in the display.

Table 305 show sccp ccm group Field Descriptions

Field	Description
CCM Group Identifier	Current state of the SCCP session.
Description	Local interface that SCCP applications use to register with Cisco Unified Communications Manager.
Binded Interface	Sets the IP precedence value for SCCP.
Registration Retries	Codec to mask.
Registration Timeout	Cisco Unified CallManager server information.
Keepalive Retries	Displays the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager.
Keepalive Timeout	Displays the number of times that a DSP farm attempts to connect to a Cisco Unified CallManager.
CCM Connect Retries	Displays the amount of time, in seconds, that a given DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
CCM Connect Interval	Method that the SCCP client uses when the communication link between the active Cisco Unified CallManager and the SCCP client fails.
Switchover Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Interval	Amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails.
Switchback Timeout	Amount of time, in seconds, that the secondary Cisco Unified CallManager waits before switching back to the primary Cisco Unified CallManager.
Associated CCM Id	Number assigned to the Cisco Unified CallManager.
Registration Name	User-specified device name in Cisco Unified CallManager.
Associated Profile	Number of the DSP farm profile associated with the Cisco Unified CallManager group.

The following sample output displays the summary information for all SCCP call references:

```
Router# show sccp call-reference
session_id: 16805277   session_type: vcf  , profile_id: 101,
    call-reference: 25666614  , Name: , Number: 3004
        Audio conn_id: 16777929  , str_passthr: 0
              rtp-call-id: 21        , bridge-id: 15        , msp-call-id: 12
              mode: sendrecv, sport: 25146, rport 16648, ripaddr: 10.22.82.205
              codec: g711u  , pkt-period: 20
    call-reference: 25666611  , Name: , Number: 6628
        Audio conn_id: 16777926  , str_passthr: 0
              rtp-call-id: 19        , bridge-id: 13        , msp-call-id: 12
              mode: sendrecv, sport: 28168, rport 2398 , ripaddr: 128.107.147.125
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777927  , conn_id_tx: 16777928  , str_passthr: 0
```

```
              rtp-call-id: 20        , bridge-id: 14        , msp-call-id: 12
              mode: sendrecv, sport: 22604, rport 2400 , ripaddr: 128.107.147.125
              bit rate: 1100kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 2.2, max mbps: 81 (x500 MB/s), max fs: 7
(x256 MBs)
    call-reference: 25666608  , Name: , Number: 62783365
        Audio conn_id: 16777923  , str_passthr: 0
              rtp-call-id: 16        , bridge-id: 11        , msp-call-id: 12
              mode: sendrecv, sport: 21490, rport 20590, ripaddr: 10.22.83.142
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777924  , conn_id_tx: 16777925  , str_passthr: 0
              rtp-call-id: 17        , bridge-id: 12        , msp-call-id: 12
              mode: sendrecv, sport: 23868, rport 29010, ripaddr: 10.22.83.142
              bit rate: 960kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 3.0, max mbps: 0 (x500 MB/s), max fs: 0
(x256 MBs)
    call-reference: 25666602  , Name: , Number: 62783363
        Audio conn_id: 16777916  , str_passthr: 0
              rtp-call-id: 11        , bridge-id: 7         , msp-call-id: 12
              mode: sendrecv, sport: 26940, rport 20672, ripaddr: 10.22.82.48
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777917  , conn_id_tx: 16777919  , str_passthr: 0
              rtp-call-id: 13        , bridge-id: 8         , msp-call-id: 12
              mode: sendrecv, sport: 16462, rport 20680, ripaddr: 10.22.82.48
              bit rate: 960kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 2.0, max mbps: 72 (x500 MB/s), max fs: 5
(x256 MBs)

Total number of active session(s) 1
   Total of number of active session(s) 1
      with total of number of call-reference(s) 4
         with total of number of audio connection(s) 4
         with total of number of video connection(s) 3
```

The following sample output displays summary information for all SCCP call identifications:

```
Router# show sccp call-identifications

sess_id   callref   conn_id   conn_id_tx spid  rtp_callid msp_callid bridge_id  codec
stype prof_id
16805277  25666614  16777929  0          0     21         12         15         g711u  vcf
101
16805277  25666611  16777926  0          0     19         12         13         g711u  vcf
101
16805277  25666611  16777927  16777928   0     20         12         14         h264   vcf
101
16805277  25666608  16777923  0          0     16         12         11         g711u  vcf
101
16805277  25666608  16777924  16777925   0     17         12         12         h264   vcf
101
16805277  25666602  16777916  0          0     11         12         7          g711u  vcf
101
16805277  25666602  16777917  16777919   0     13         12         8          h264   vcf
101

Total number of active session(s) 1
```

The following sample displays the output from **show sccp**:

```
Router# show sccp

SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/1
        IPv4 Address: 172.19.156.7
        Port Number: 2000
```

```
IP Precedence: 5
User Masked Codec list: None
Call Manager: 1.4.211.39, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 1
                Trustpoint: N/A
Call Manager: 128.107.151.39, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 100
                Trustpoint: N/A

V_Conferencing Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 128.107.151.39, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 101
Reported Max Streams: 4, Reported Max OOS Streams: 0
Layout: default 1x1
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
Supported Codec: g729r8, Maximum Packetization Period: 60
Supported Codec: g729br8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30
Supported Codec: h264: QCIF, Frame Rate: 15fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: QCIF, Frame Rate: 30fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: CIF, Frame Rate: 15fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: CIF, Frame Rate: 30fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: 4CIF, Frame Rate: 30fps, Bit Rate: 1000-1000 Kbps
TLS : ENABLED
```

Related Commands

Command	Description
dsp service dspfarm	Configures DSP farm services for a specified voice card.
dspfarm (DSP farm)	Enables DSP-farm service.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show dspfarm	Displays summary information about DSP resources.

show sip-ua calls

To display active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (SIP) calls, use the **show sip-ua calls** command in privileged EXEC mode.

show sip-ua calls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(22)T	Command output was updated to show IPv6 information and to display Resource Reservation Protocol (RSVP) quality of service (QoS) preconditions information.

Usage Guidelines

The **show sip-ua calls** command displays active UAC and UAS information for SIP calls on a Cisco IOS device. The output includes information about IPv6, RSVP, and media forking for each call on the device and for all media streams associated with the calls. There can be any number of media streams associated with a call, of which typically only one is active. However, a call can include up to three active media streams if the call is media-forked. Use this command when debugging multiple media streams to determine if an active call on the device is forked.

Examples

The following is sample output from the **show sip-ua calls** command for a forked call with four associated media streams, three of which are currently active:

```
Router# show sip-ua calls

SIP UAC CALL INFO

Call 1
SIP Call ID : 515205D4-20B711D6-8015FF77-1973C402@172.18.195.49
 State of the call : STATE_ACTIVE (6)
 Substate of the call : SUBSTATE_NONE (0)
 Calling Number : 5550200
 Called Number : 5551101
 Bit Flags : 0x12120030 0x220000
 Source IP Address (Sig ): 172.18.195.49
 Destn SIP Req Addr:Port : 172.18.207.18:5063
 Destn SIP Resp Addr:Port: 172.18.207.18:5063
 Destination Name : 172.18.207.18
 Number of Media Streams : 4
 Number of Active Streams: 3
 RTP Fork Object : 0x637C7B60
 Media Stream 1
  State of the stream : STREAM_ACTIVE
  Stream Call ID : 28
  Stream Type : voice-only (0)
  Negotiated Codec : g711ulaw (160 bytes)
  Codec Payload Type : 0
  Negotiated Dtmf-relay : inband-voice
```

```
  Dtmf-relay Payload Type : 0
  Media Source IP Addr:Port: 172.18.195.49:19444
  Media Dest IP Addr:Port : 172.18.193.190:16890
 Media Stream 2
  State of the stream : STREAM_ACTIVE
  Stream Call ID : 33
  Stream Type : voice+dtmf (1)
  Negotiated Codec : g711ulaw (160 bytes)
  Codec Payload Type : 0
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  Media Source IP Addr:Port: 172.18.195.49:18928
  Media Dest IP Addr:Port : 172.18.195.73:18246
 Media Stream 3
  State of the stream : STREAM_ACTIVE
  Stream Call ID : 34
  Stream Type : dtmf-only (2)
  Negotiated Codec : No Codec (0 bytes)
  Codec Payload Type : -1 (None)
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  Media Source IP Addr:Port: 172.18.195.49:18428
  Media Dest IP Addr:Port : 172.16.123.99:34463
 Media Stream 4
  State of the stream : STREAM_DEAD
  Stream Call ID : -1
  Stream Type : dtmf-only (2)
  Negotiated Codec : No Codec (0 bytes)
  Codec Payload Type : -1 (None)
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  Media Source IP Addr:Port: 172.18.195.49:0
  Media Dest IP Addr:Port : 172.16.123.99:0

 Number of UAC calls: 1

SIP UAS CALL INFO

 Number of UAS calls: 0
```

The following is sample output from the **show sip-ua calls** command showing IPv6 information:

```
Router# show sip-ua calls

SIP UAC CALL INFO

Call 1
SIP Call ID                : 8368ED08-1C2A11DD-80078908-BA2972D0@2001::21B:D4FF:FED7:B000
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 2000
   Called Number           : 1000
   Bit Flags               : 0xC04018 0x100 0x0
   CC Call ID              : 2
   Source IP Address (Sig ): 2001::21B:D4FF:FED7:B000
   Destn SIP Req Addr:Port : [2001::21B:D5FF:FE1D:6C00]:5060
   Destn SIP Resp Addr:Port: [2001::21B:D5FF:FE1D:6C00]:5060
   Destination Name        : 2001::21B:D5FF:FE1D:6C00
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
```

```
     Stream Call ID           : 2
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1709707780
     Negotiated Codec         :  (20 bytes)
     Codec Payload Type       : 18
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     Media Source IP Addr:Port: [2001::21B:D4FF:FED7:B000]:16504
     Media Dest IP Addr:Port  : [2001::21B:D5FF:FE1D:6C00]:19548

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO

   Number of SIP User Agent Server(UAS) calls: 0
```

The following is sample output from the **show sip-ua calls** command when mandatory QoS is configured at both endpoints and RSVP has succeeded:

```
Router# show sip-ua calls

SIP UAC CALL INFO

  Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : F31FEA20-CFF411DC-8068DDB4-22C622B8@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:64440
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:18542
  Media Dest IP Addr:Port  : 172.18.19.73:16912
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Mandatory
  Negotiated QoS Strength  : Mandatory
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success


Options-Ping    ENABLED:NO     ACTIVE:NO
 Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when optional QoS is configured at both endpoints and RSVP has succeeded:

```
Router# show sip-ua calls

SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Optional
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when optional QoS is configured at both endpoints and RSVP has failed:

```
Router# show sip-ua calls

SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
```

```
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Optional
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Fail

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when the command is used on the originating gateway (OGW) while optional QoS is configured on the OGW, mandatory QoS is configured on the terminating gateway (TGW), and RSVP has succeeded:

```
Router# show sip-ua calls

SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
```

```
  Stream Type               : voice-only (0)
  Negotiated Codec          : g711ulaw (160 bytes)
  Codec Payload Type        : 0
  Negotiated Dtmf-relay     : inband-voice
  Dtmf-relay Payload Type   : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port   : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                    : -2
  Local QoS Strength        : Optional
  Negotiated QoS Strength   : Mandatory
  Negotiated QoS Direction : SendRecv
  Local QoS Status          : Success

Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

Table 267 describes the significant fields shown in the displays.

Table 306 show sip-ua calls Field Descriptions

Field	Description
SIP UAC CALL INFO	Field header that indicates that the following information pertains to the SIP UAC.
Call 1	Field header.
SIP Call ID	UAC call identification number.
State of the call	Indicates the state of the call. This field is used for debugging purposes. The state is variable and may be different from one Cisco IOS release to another.
Substate of the call	Indicates the substate of the call. This field is used for debugging purposes. The state is variable and may be different from one Cisco IOS release to another.
Calling Number	Indicates the calling number.
Called Number	Indicates the called number.
Bit Flags	Indicates the bit flags used for debugging.
Source IP Address (Sig)	Indicates the signaling source IPv4 or IPv6 address.
Destn SIP Req Addr: Port:	Indicates the signaling destination Request IPv4 or IPv6 address and port number.
Destn SIP Resp Addr: Port:	Indicates the signaling destination Response IPv4 or IPv6 address and port number.
Destination Name	Indicates the signaling destination hostname, IPv4 address, or IPv6 address.
Number of Media Streams	Indicates the total number of media streams for this UAC call.
Number of Active Streams:	Indicates the total number of active media streams.
RTP Fork Object	Pointer address of the internal RTP Fork data structure.
Media Stream	Statistics about each active media stream are reported. The Media Stream header indicates the number of the media stream, and its statistics immediately follow this header.

Table 306 show sip-ua calls Field Descriptions (continued)

Field	Description
State of the stream	State of the media stream indicated by the Media Stream header. Can be STREAM_ACTIVE, STREAM_ADDING, STREAM_CHANGING, STREAM_DEAD, STREAM_DELETING, STREAM_IDLE, or Invalid Stream State.
Stream Call ID	Identification of the stream call indicated by the Media Stream header.
Stream Type	Type of stream indicated by the Media Stream header. It can be dtmf-only, dtmf-relay, voice-only, or voice+dtmf-relay.
Negotiated Codec	Codec selected for the media stream. It can be g711ulaw, <G.729>, <G.726>, or No Codec.
Codec Payload Type	Payload type of the Negotiated Codec.
Negotiated Dtmf-relay	DTMF relay selected for the media stream indicated by the Media Stream header. It can be inband-voice or rtp-nte.
Dtmf-relay Payload Type	Payload type of the negotiated DTMF relay.
Media Source IP Addr: Port	The source IPv4 or IPv6 address and port number of the media stream indicated by the Media Stream header.
Media Dest IP Addr: Port	The destination IPv4 or IPv6 address and port number of the media stream indicated by the Media Stream header.
Local QoS Strength	The QoS strength (mandatory or optional) configured for this device.
Negotiated QoS Strength	The QoS strength (mandatory or optional) that has been negotiated.
Negotiated QoS Direction	Displays the direction in which RSVP was negotiated. For example, sendrecv indicates that RSVP was negotiated in both directions.
Local QoS Status	Displays the success or failure of RSVP reservation.
Number of UAC calls	Final SIP UAC CALL INFO field. Indicates the number of UAC calls.
SIP UAS CALL INFO	Field header that indicates that the following information pertains to the SIP UAS.
Number of UAS calls	Final SIP UAS CALL INFO field. Indicates the number of UAS calls.

Related Commands

Command	Description
debug ccsip all	Enables all SIP-related debugging.
debug ccsip events	Enablestracing of events that are specific to SIP SPI.
debug ccsip info	Enables tracing of general SIP SPI information.
debug ccsip media	Enables tracing of SIP call media streams.
debug ccsip messages	Enables tracing of SIP Service Provider Interface (SPI) messages.

show sip-ua connections

To display Session Initiation Protocol (SIP) user-agent (UA) transport connection tables, use the **show sip-ua connections** command in privileged EXEC mode.

show sip-ua connections {**tcp** [**tls**] | **udp**} {**brief** | **detail**}

Syntax Description

tcp	Displays all TCP connection information.
tls	(Optional) Displays all Transport Layer Security (TLS) over TCP connection information.
udp	Displays all User Datagram Protocol (UDP) connection information.
brief	Displays a summary of connections.
detail	Displays detailed connection information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced
12.4(6)T	The optional **tls** keyword was added.
12.4(22)T	Command output was updated to show IPv6 information.
15.1(2)T	The command output was updated to display the SIP socket listeners information.

Usage Guidelines

The **show sip-ua connections** command should be executed only after a call is made. Use this command to learn the connection details.

Examples

The following sample output from this command shows multiple calls to multiple destinations. Although this example shows UDP details, the command output looks identical for TCP calls.

```
Router# show sip-ua connections udp detail

Total active connections : 2
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
```

```
=========== ======= =========== ===========
5060 1 Established 0
Remote-Agent:172.19.154.18, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060        2       Established   0

Router# show sip-ua connections tcp detail

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060         1      Established   0

Router# show sip-ua connections udp detail

Total active connections      : 1
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:2001:DB8:C18:4:21D:E5FF:FE34:26A0, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address
  =========== ======= =========== =========== ===========
         5060       2 Established           0  -

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id               Local-Address
 ===========    ============================
   0            [0.0.0.0]:5060
   2            [8.6.8.8]:5060

Router# show sip-ua connections tcp tls brief

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
```

```
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id                Local-Address
 ===========    ============================
   0            [0.0.0.0]:5061
```

The following is sample output from the **show sip-ua connections** command showing IPv6 information:

```
Router# show sip-ua connections udp brief

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 10

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id                Local-Address
 ===========    ============================
   0            [0.0.0.0]:5060
```

Table 307 describes the significant fields shown in the display.

Table 307 show sip-ua connections Field Descriptions

Field	Description
Total active connections	Indicates all the connections that the gateway holds for various targets. Statistics are broken down within individual fields.
No. of send failures	Indicates the number of TCP or UDP messages dropped by the transport layer. Messages are dropped if there were network issues, and the connection was frequently ended.
No. of remote closures	Indicates the number of times a remote gateway ended the connection. A higher value indicates a problem with the network or that the remote gateway does not support reusing the connections (thus it is not RFC 3261-compliant). The remote closure number can also contribute to the number of send failures.
No. of conn. failures	Indicates the number of times that the transport layer was unsuccessful in establishing the connection to the remote agent. The field can also indicate that the address or port configured under the dial peer might be incorrect or that the remote gateway does not support that mode of transport.
No. of inactive conn. ageouts	Indicates the number of times that the connections were ended or timed out because of signaling inactivity. During call traffic, this number should be zero. If it is not zero, we recommend that the inactivity timer be tuned to optimize performance by using the **timers** command.
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0	Indicates the number of messages waiting in the queue to be sent out on the TCP connection when the congestion was at its peak. A higher queue number indicates that more messages are waiting to be sent on the network. The growth of this queue size cannot be controlled directly by the administrator.

Table 307 show sip-ua connections Field Descriptions (continued)

Field	Description
Tuples with no matching socket entry	Any tuples for the connection entry that are marked with "**" at the end of the line indicate an upper transport layer error condition; specifically, that the upper transport layer is out of sync with the lower connection layer. Cisco IOS software should automatically overcome this condition. If the error persists, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection** command and report the problem to your support team.
Tuples with mismatched address/port entry	Any tuples for the connection entry that are marked with “++” at the end of the line indicate an upper transport layer error condition, where the socket is probably readable, but is not being used. If the error persists, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection** command and report the problem to your support team.
Remote-Agent Connections-Count	Connections to the same target address. This field indicates how many connections are established to the same host.
Remote-Port Conn-Id Conn-State WriteQ-Size	Connections to the same target address. This field indicates how many connections are established to the same host. The WriteQ-Size field is relevant only to TCP connections and is a good indicator of network congestion and if there is a need to tune the TCP parameters.

Related Commands

Command	Description
clear sip-ua tcp connection	Clears a SIP TCP connection.
clear sip-ua udp connection	Clears a SIP UDP connection.
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP user agent status.
show sip-ua timers	Displays the current settings for the SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.
timers	Configures the SIP signaling timers.

show sip-ua status

To display status for the Session Initiation Protocol (SIP) user agent (UA), use the **show sip-ua status** command in privileged EXEC mode.

show sip-ua status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	The statistics portion of the output was removed and included in the **show sip-ua statistics** command.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	Command output was enhanced to display if media or signaling binding is enabled, and the style of the DNS SRV query (1 for RFC 2052; 2 for RFC 2782).
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua** command.
12.2(11)T	Command output was enhanced to display information on Session Description Protocol (SDP) application configuration. This command was supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(13)T	Command output was enhanced to display the following: Information on redirection message handling. Information on handling of 180 responses with SDP.
12.2(15)T	Command output was enhanced to display Suspend and Resume support.
12.2(15)ZJ	Command output was enhanced to display information on the duration of dual-tone multifrequency (DTMF) events.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	Command output was enhanced to display Reason Header support.
12.4(22)T	Command output was updated to show IPv6 information.
Cisco IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use this command to verify SIP configurations.

Examples

The following is sample output from the **show sip-ua status** command:

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED

SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv4

SDP application configuration:
 Version line (v=) required
 Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

The following is sample output from the **show sip-ua status** command showing IPv6 information:

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED

SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv6

SDP application configuration:
 Version line (v=) required
Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
```

```
Network types supported: IN
Address types supported: IP4 IP6
Transport types supported: RTP/AVP udptl
```

Table 308 describes the significant fields shown in the display.

Table 308 show sip-ua status Field Descriptions

Field	Description
SIP User Agent Status	UA status.
SIP User Agent for UDP	User Datagram Protocol (UDP) is enabled or disabled.
SIP User Agent for TCP	TCP is enabled or disabled.
SIP User Agent bind status (signaling)	Binding for signaling is enabled or disabled.
SIP User Agent bind status (media)	Binding for media is enabled or disabled.
SIP early-media for 180 responses with SDP	Early media cut-through treatment for 180 responses with SDP can be enabled (the default treatment) or disabled, with local ringback provided.
SIP max-forwards	Value of max-forwards of SIP messages.
SIP DNS SRV version	Style of the DNS SRV query: 1 for RFC 2052 or 2 for RFC 2782.
NAT Settings for the SIP-UA	Symmetric Network Address Translation (NAT) settings when the feature is enabled.
Role in SDP	Identifies the endpoint function in the connection setup procedure during symmetric NAT traversal. The endpoint role may be set to active, meaning that it initiates a connection, or to passive, meaning that it accepts a connection. A value of none in this field means that the feature is disabled.
Check media source packets	Media source packet checking is enabled or disabled.
Maximum duration for a telephone-event in NOTIFYs	Shows the time interval, in milliseconds (ms), between consecutive NOTIFY messages for a telephone event.
SIP support for ISDN SUSPEND/RESUME	Suspend and Resume support is enabled or disabled.
Redirection (3xx) message handling	Redirection can be enabled, which is the default status, according to RFC 2543. Or handling of redirection 3*xx* messages can be disabled, allowing the gateway to treat 3*xx* redirect messages as 4*xx* error messages.
Reason Header will override Response/Request Codes	Reason header is enabled or disabled.
protocol mode is ipv6	States whether the protocol being used is IPv6 or IPv4.
Version line (v=)	Indicates if the SDP version is required.
Owner line (o=)	Indicates if the session originator is required.
Timespec line (t=)	Indicates if the session start and stop times are required.
Media supported	Media information.
Network types supported	Always IN for Internet.

Table 308 show sip-ua status Field Descriptions (continued)

Field	Description
Address types supported	Identifies the Internet Protocol version.
Transport types supported	Identifies the transport protocols supported.

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby** command in user EXEC or privileged EXEC mode.

show standby [*type number* [*group*]] [**all** | **brief**]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.
group	(Optional) Group number on the interface for which output is displayed.
all	(Optional) Displays information for groups that are learned or do not have the **standby ip** command configured.
brief	(Optional) A single line of output summarizes each standby group.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	The output for the command was made clearer and easier to understand.
12.3(2)T	The output was enhanced to display information about Message Digest 5 (MD5) authentication.
12.3(4)T	The output was enhanced to display information about HSRP version 2.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(4)T	IPv6 support was added.
12.4(6)T	The output for this command was enhanced to display information about HSRP master and client groups.
12.4(9)T	The output for this command was enhanced to display information about HSRP group shutdown configuration.
12.4(11)T	The output for this command was enhanced to display information about HSRP Bidirectional Forwarding Detection (BFD) peering.
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.
12.2(33)SXI	The output for this command was enhanced to display information about gratuitous ARP packets.
12.4(24)T	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
12.2(33)SXI1	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Release	Modification
Cisco IOS XE Release 2.4	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
12.2(33)SRE	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.

Usage Guidelines

To specify a group, you must specify an interface type and number.

Examples

The following is sample output from the **show standby** command:

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
   2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
   Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
   Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
   Next hello sent in 1.412 secs
  Gratuitous ARP 14 sent, next in 7.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
   Tracking 2 objects, 0 up
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
Group name is “HSRP1” (cfgd)
Follow by groups:
    Et1/0.3 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs (next 19.666)
    Et1/0.4 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs (next 19.491)
  Group name is "HSRP1", advertisement interval is 34 sec
```

The following is sample output from the **show standby** command when HSRP version 2 is configured:

```
Router# show standby

Ethernet0/1 - Group 1 (version 2)
  State is Speak
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is unknown
   Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
   Next hello sent in 1.804 secs

  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 20 (configured 20)
  Group name is "hsrp-Et0/1-1" (default)

Ethernet0/2 - Group 1
  State is Speak
  Virtual IP address is 10.22.0.10
  Active virtual MAC address is unknown
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
```

```
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.804 secs
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 90 (default 100)
    Track interface Serial2/0 state Down decrement 10
  Group name is "hsrp-Et0/2-1" (default)
```

The following is sample output from the **show standby** command with the **brief** keyword specified:

```
Router# show standby brief

Interface   Grp Prio P State    Active addr     Standby addr    Group addr
Et0         0   120    Init     10.0.0.1        unknown         10.0.0.12
```

The following is sample output from the **show standby** command when HSRP MD5 authentication is configured:

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
    5 state changes, last state change 00:17:27
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.276 secs
  Authentication MD5, key-string, timeout 30 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Et0/1-1" (default)
```

The following is sample output from the **show standby** command when HSRP group shutdown is configured:

```
Router# show standby

Ethernet0/0 - Group 1
State is Init (tracking shutdown)
3 state changes, last state change 00:30:59
Track object 100 state Up
Track object 101 state Down
Track object 103 state Up
```

The following is sample output from the **show standby** command when HSRP BFD peering is enabled:

```
Router# show standby

Ethernet0/0 - Group 2
  State is Listen
    2 state changes, last state change 01:18:18
  Virtual IP address is 10.0.0.1
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption enabled
  Active router is 10.0.0.250, priority 120 (expires in 9.396 sec)
  Standby router is 10.0.0.251, priority 110 (expires in 8.672 sec)
    BFD enabled
  Priority 90 (configured 90)
```

```
  Group name is "hsrp-Et0/0-1" (default)
```

The following is sample output from the **show standby** command used to display the state of the standby RP:

```
Router# show standby

GigabitEthernet3/25 - Group 1
State is Init (standby RP, peer state is Active)
Virtual IP address is 10.0.0.1
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption disabled
Active router is unknown
Standby router is unknown
Priority 100 (default 100)
Group name is "hsrp-Gi3/25-1" (default)
```

Table 309 describes the significant fields shown in the displays.

Table 309 show standby Field Descriptions

Field	Description
Ethernet - Group	Interface type and number and Hot Standby group number for the interface.
State is	State of local router; can be one of the following: • Active—Indicates the current Hot Standby router. • Standby—Indicates the router next in line to be the Hot Standby router. • Speak—Router is sending packets to claim the active or standby role. • Listen—Router is neither in the active nor standby state, but if no messages are received from the active or standby router, it will start to speak. • Init or Disabled—Router is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other routers on the network that are learned via snooping are displayed as being in the Init state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state. For these cases, the Active addr and Standby addr fields will show "unknown." The state is listed as disabled in the fields when the **standby ip** command has not been specified. • Init (tracking shutdown)—HSRP groups appear in the Init state when HSRP group shutdown has been configured and a tracked object goes down.
Virtual IP address is, Secondary virtual IP addresses	All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as "duplicate." A duplicate address indicates that the router has failed to defend its ARP (Address Resolution Protocol) cache entry.
Active virtual MAC address	Virtual MAC address being used by the current active router.
Local virtual MAC address	Virtual MAC address that would be used if this router became the active router. The origin of this address (displayed in parentheses) can be "default," "bia," (burned-in address) or "confgd" (configured).

Table 309 show standby Field Descriptions (continued)

Field	Description
Hello time, hold time	The hello time is the time between hello packets (in seconds) based on the command. The holdtime is the time (in seconds) before other routers declare the active or standby router to be down, based on the **standby timers** command. All routers in an HSRP group use the hello and hold- time values of the current active router. If the locally configured values are different, the variance appears in parentheses after the hello time and hold-time values.
Next hello sent in	Time in which the Cisco IOS software will send the next hello packet (in hours:minutes:seconds).
Gratuitous ARP 14 sent, next in 7.412 secs	Number of the gratuitous ARP packet HSRP has sent and the time in seconds when HSRP will send the next gratuitous ARP packet. This output appears only when HSRP sends gratuitous ARP packets.
Authentication	Authentication type configured based on the **standby authentication** command.
key-string	Indicates a key string is used for authentication. Configured key chains are not displayed.
timeout	Duration (in seconds) that HSRP will accept message digests based on both the old and new keys.
Preemption enabled, sync delay	Indicates whether preemption is enabled. If enabled, the minimum delay is the time a higher-priority nonactive router will wait before preempting the lower-priority active router. The sync delay is the maximum time a group will wait to synchronize with the IP redundancy clients.
Active router is	Value can be “local,” “unknown,” or an IP address. Address (and the expiration date of the address) of the current active Hot Standby router.
Standby router is	Value can be “local,” “unknown,” or an IP address. Address (and the expiration date of the address) of the “standby” router (the router that is next in line to be the Hot Standby router).
BFD enabled	Indicates that BFD peering is enabled on the router.
expires in	Time (in hours:minutes:seconds) in which the standby router will no longer be the standby router if the local router receives no hello packets from it.
Tracking	List of interfaces that are being tracked and their corresponding states. Based on the **standby track** command.
Group name is	The name of the HSRP group.
Follow by groups:	Indicates the client HSRP groups that have been configured to follow this HSRP group.
P	Indicates that the router is configured to preempt.

Related Commands

Command	Description
standby authentication	Configures an authentication string for the HSRP.
standby ip	Activates the HSRP.
standby mac-address	Specifies the virtual MAC address for the virtual router.
standby mac-refresh	Refreshes the MAC cache on the switch by periodically sending packets from the virtual MAC address.

Command	Description
standby preempt	Configures HSRP preemption and preemption delay.
standby priority	Configures Hot Standby priority of potential standby routers.
standby timers	Configures the time between hello messages and the time before other routers declare the active Hot Standby or standby router to be down.
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
standby use-bias	Configures HSRP to use the BIA of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring).

show stcapp device

To display configuration information about Skinny Client Control Protocol (SCCP) telephony control (STC) application (STCAPP) analog voice ports, use the **show stcapp device** command in privileged EXEC mode.

show stcapp device {**name** *device-name* | **summary** | **voice-port** *port*}

Syntax Description

name *device-name*	Displays information for the analog voice port with the specified device name. The device name is the unique device ID that is assigned to the port when it registers with the call-control system.
summary	Displays a summary of all voice ports.
voice-port *port*	Displays information for the specified analog voice port. **Note** The *port* syntax is platform-dependent; type ? to determine appropriate port numbering.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	This command was modified. Command output was enhanced to display call control block (CCB) and call-control device information.
12.4(4)T	This command was modified. Command output was enhanced to display supported modem transport capability.
12.4(6)XE	This command was modified. Command output was enhanced to display visual message waiting indicator (VMWI) and information for Dial Tone After Remote Onhook feature.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.
15.0(1)XA	This command was modified. Cancel Call Waiting information was added to the command output.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. Command output was enhanced to display the call waiting tone configuration.

Usage Guidelines

Use this command to display configuration and voice interface card (VIC)-specific port information. The Active Call Info field is populated only if a call is active on the voice port.

Examples

The following is a sample output showing IPv6 addresses for the local and remote sites:

```
Router# show stcapp device voice-port 2/0

Port Identifier: 2/0
Device Type: ALG
Device Id: 1
Device Name: AN1AE2853624400
Device Security Mode : None
Modem Capability: None
Device State: IS
Diagnostic: None
Directory Number: 1000
Dial Peer(s): 1000
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event: STCAPP_DC_EV_DEVICE_CALL_INFO
Line State: ACTIVE
Hook State: OFFHOOK
mwi: DISABLE
vmwi: OFF
PLAR: DISABLE
Number of CCBs: 1
Global call info:
Total CCB count = 2
Total call leg count = 4

Call State for Connection 1: TsConnected
Connected Call Info:
Call Reference: 22690511
Local IPv6 Addr: 2001:DB8:C18:1:218:FEFF:FE71:2AB6
Local IP Port: 17424
Remote IPv6 Addr: 2001:DB8:C18:1:218:FEFF:FE71:2AB6
Remote IP Port: 18282
Calling Number: 1000
Called Number:
Codec: g729br8
SRTP: off
```

The following is a sample output from the **show stcapp device** command for an SCCP analog port with VMWI while the Dial Tone After Remote Onhook Feature is activated:

```
Router# show stcapp device voice-port 2/4
Port Identifier:  2/4
Device Type:      ALG
Device Id:        4
Device Name:      AN0C863967C9404
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 7204
Dial Peer(s):     4
Dialtone after remote onhook feature: activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Hook State:       ONHOOK
mwi:              ENABLE
vmwi:             ON
PLAR:             DISABLE
Number of CCBs:   0
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port on a VIC2-2FXS voice interface card specified by the port number:

```
Router# show stcapp device voice-port 1/0/0

Port Identifier:  1/0/0
Device Type:      ALG
Device Id:        3
Device Name:      AN1EBEEB6070200
Device Security Mode : None
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 2099
Dial Peer(s):     999100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
ccw_on:           FALSE
mwi:              DISABLE
vmwi:             OFF
PLAR:             DISABLE
Callback State:   DISABLED
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
    Total call leg count = 0
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port:

```
Router# show stcapp device name AN0C863972F5401

Port Identifier:  2/1
Device Type:      ALG
Device Id:        25
Device Name:      AN0C863972F5401
Device State:     IS
Diagnostic:       None
Directory Number: 9101
Dial Peer(s):     2
Last Event:       STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:       ACTIVE
Hook State:       OFFHOOK
Number of CCBs:   1
Global call info:
    Total CCB count      = 3
    Total call leg count = 6

Call State for Connection 1: TsConnected
Connected Call Info:
   Call Reference: 16777509
   Local IP Addr:  10.1.0.1
   Local IP Port:  18768
   Remote IP Addr: 10.1.0.1
   Remote IP Port: 18542
   Calling Number: 9101
   Called Number:  9102
   Codec:          g711ulaw
```

The following is a sample output from the **show stcapp device** command for STCAPP analog voice ports:

```
Router# show stcapp device summary

Total Devices:           24
Total Calls in Progress: 3
Total Call Legs in Use:  6

Port       Device          Device   Call          Dev  Directory   Dev
Identifier Name            State    State         Type Number      Cntl
---------- --------------- -------- ------------- ---- ----------- ----
2/1        AN0C863972F5401 IS       ACTIVE         ALG  9101       CCM
2/2        AN0C863972F5402 IS       ACTIVE         ALG  9102       CCM
2/3        AN0C863972F5403 IS       ACTIVE         ALG  9103       CCM
2/0        AN0C863972F5400 IS       IDLE           ALG  9100       CCM
2/4        AN0C863972F5404 IS       IDLE           ALG  9104       CCM
2/5        AN0C863972F5405 IS       IDLE           ALG  9105       CCM
2/6        AN0C863972F5406 IS       IDLE           ALG  9106       CCM
2/7        AN0C863972F5407 IS       IDLE           ALG  9107       CCM
2/8        AN0C863972F5408 IS       IDLE           ALG  9108       CCM
2/9        AN0C863972F5409 IS       IDLE           ALG  9109       CCM
2/10       AN0C863972F540A IS       IDLE           ALG  9110       CCM
2/11       AN0C863972F540B IS       IDLE           ALG  9111       CCM
2/12       AN0C863972F540C IS       IDLE           ALG  9112       CCM
2/13       AN0C863972F540D IS       IDLE           ALG  9113       CCM
2/14       AN0C863972F540E IS       IDLE           ALG  9114       CCM
2/15       AN0C863972F540F IS       IDLE           ALG  9115       CCM
2/16       AN0C863972F5410 IS       IDLE           ALG  9116       CCM
2/17       AN0C863972F5411 IS       IDLE           ALG  9117       CCM
2/18       AN0C863972F5412 IS       IDLE           ALG  9118       CCM
2/19       AN0C863972F5413 IS       IDLE           ALG  9119       CCM
2/20       AN0C863972F5414 IS       IDLE           ALG  9120       CCM
2/21       AN0C863972F5415 IS       IDLE           ALG  9121       CCM
2/22       AN0C863972F5416 IS       IDLE           ALG  9122       CCM
2/23       AN0C863972F5417 IS       IDLE           ALG  9123       CCM
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port:

```
Router# show stcapp device name AN0C86385E3D400

Port Identifier: 2/0
Device Type:      ALG
Device Id:        1
Device Name:      AN0C86385E3D400
Device Security Mode : None
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 2400
Dial Peer(s):     2000
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
mwi:              DISABLE
vmwi:             OFF
mwi config:       Both
Privacy:          Not configured
PLAR:             DISABLE
Callback State:   IDLE
```

```
CWT Repetition Interval: 0 second(s)
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
    Total call leg count = 0
```

Table 310 describes the significant fields shown in these displays, in alphabetical order.

Table 310 show stcapp device Field Descriptions

Field	Description
Active Call Info	Displays only when an active call is in progress.
Call Reference	Reference number created by Cisco Unified Communications Manager to track messages associated with a specific call.
Call State	Call processing state: • ACTIVE—Established call connection • IDLE—No call connection • UNREGISTERED—Device is not registered with the Cisco Unified Communications Manager
Called Number	Device called number.
Calling Number	Device calling number.
ccw_on	Displays status of Cancel Call Waiting feature: • False—Inactive on port. • True—Active on port.
Codec	Displays codec type.
CWT Repetition Interval	Displays the call waiting tone configuration.
Dev Cntl	Call-control device that is managing the analog endpoints. CCM represents Cisco Unified Communications Manager. CME represents Cisco Unified Communications Manager Express.
Device Id	Identifier used between the Cisco Unified Communications Manager and gateway to uniquely identify an endpoint.
Device Name	Unique device ID of the analog endpoint. The device ID is derived from an algorithm using the MAC address of the SCCP interface on the voice gateway and the hexadecimal translation of the port's slot number and port number.

Table 310 show stcapp device Field Descriptions (continued)

Field	Description
Device State	Displays whether device is available for use: • ACTIVE_PENDING—Call is pending certain events before going active. • INFO_RCVD—Call information is received from the Cisco Unified Communications Manager during call setup. • INIT—Waiting to reinitialize. • IS—In service. • OFFHOOK—Device is off-hook. • OFFHOOK_TIMEOUT—Digit timeout occurred while the device is off-hook. • ONHOOK_PENDING—Call is pending certain events before going to the on-hook state. • OOS—Out of service. • PROCEED—Dialed number translation is complete and call setup is in progress. • REM_ONHOOK_PENDING—Call is pending certain events before going to the on-hook state. • RINGING—An incoming call has invoked ringing of the receiving device.
Device Type	Shows phone type: • ALG—Analog. • BRI—ISDN BRI.
Diagnostic	Reason code for a device error condition.
Dial Peer(s)	Dial peer name.
Dialtone after remote onhook feature	Displays feature status: • Activated • Not activated
Directory Number	Assigned to the device by the Cisco Unified Communications Manager.
Last Event	Last event processed by this port.
Local IP Addr	IPv4 address of this gateway used to stream audio using the Real-Time Transport Protocol (RTP).
Local IPv6 Addr	IPv6 address of this gateway used to stream audio using the RTP.
Local IP Port	IP port of this gateway used to stream audio using RTP.
Port Identifier	Identifies the physical voice port.
Remote IP Addr	IPv4 address of the far-end gateway that streams audio using RTP.
Remote IPv6 Addr	IPv6 address of the far-end gateway that streams audio using RTP.

Table 310 show stcapp device Field Descriptions (continued)

Field	Description
Remote IP Port	IP port of the far-end gateway that streams audio using RTP.
vmwi	Displays LED status: • On • Off

Related Commands

Command	Description
show stcapp statistics	Displays call statistics for STCAPP devices.

show trace multilink

To display information about multilink Frame Relay (MFR) issues, use the s**how trace multilink** command in privileged EXEC mode.

show trace multilink [**clear** | **continuous** | **detail** | **display** | **filter** | **last** | **resume** | **size** | **stop**]

Syntax Description

clear	(Optional) Value used to clear the trace buffer.
continuous	(Optional) Value that allows the trace to be shown continuously.
detail	(Optional) Value that provides trace detail.
display	(Optional) Value that control display options.
filter	(Optional) Value used to specify a filter.
last	(Optional) Value used to display the last several issues.
resume	(Optional) Value used to resume tracing.
size	(Optional) Trace buffer size, in bytes.
stop	(Optional) Value used to stop tracing.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(33)S	This command was introduced on the Cisco 12000 Series Routers.

Usage Guidelines

The **show trace multilink** command is useful in tracking what events happened when multilink Frame Relay goes up or goes down. The CLI is a debug tool used to collect the event logs pertaining to multilink feature. This command can be issued on the Router Processor Card (RP) and on individual line cards (LC) in the Cisco IOS 12000 series.

Examples

The following example enables the **show trace multilink** command:

```
Router# show trace multilink
```

show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

show track [*object-number* [**brief**] | **interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

Syntax Description

object-number	(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.
interface	(Optional) Displays tracked interface objects.
ip route	(Optional) Displays tracked IP-route objects.
resolution	(Optional) Displays resolution of tracked parameters.
timers	(Optional) Displays polling interval timers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(8)T	The output was enhanced to include the track-list objects.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(2)T	The output was enhanced to display stub objects.
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	This command was enhanced to display information about the status of an interface when carrier-delay detection has been enabled.
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.
12.4(20)T	The output was enhanced to display IP SLAs information.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

Use this command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows information about the state of IP routing on the interface that is being tracked:

```
Router# show track 1

Track 1
 Interface Ethernet0/2 ip routing
 IP routing is Down (no IP addr)
  1 change, last change 00:01:08
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows information about the line-protocol state on the interface that is being tracked:

```
Router# show track 1

Track 1
 Interface Ethernet0/1 line-protocol
 Line protocol is Up
  1 change, last change 00:00:05
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows information about the reachability of a route that is being tracked:

```
Router# show track 1

Track 1
 IP route 10.16.0.0 255.255.0.0 reachability
 Reachability is Up (RIP)
  1 change, last change 00:02:04
 First-hop interface is Ethernet0/1
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows information about the threshold metric of a route that is being tracked:

```
Router# show track 1

Track 1
 IP route 10.16.0.0 255.255.0.0 metric threshold
 Metric threshold is Up (RIP/6/102)
  1 change, last change 00:00:08
 Metric threshold down 255 up 254
 First-hop interface is Ethernet0/1
 Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows the object type, the interval in which it is polled, and the time until the next poll:

```
Router# show track timers

 Object type   Poll Interval  Time to next poll
 interface     1              expired
```

```
 ip route      30             29.364
```

The following example shows the state of the IP SLAs tracking:

```
Router# show track 50

Track 50
  IP SLA 400 state
  State is Up
    1 change, last change 00:00:23
  Delay up 60 secs, down 30 secs
  Latest operation return code: Unknown
```

The following example shows whether a route is reachable:

```
Router# show track 3

Track 3
   IP SLA 1 reachability
   Reachability is Up
     1 change, last change 00:00:47
   Latest operation return code: over threshold
   Latest RTT (millisecs) 4
   Tracked by:
     HSRP Ethernet0/1 3
```

Table 311 describes the significant fields shown in the displays.

Table 311 show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface Ethernet0/2 ip routing	Interface type, interface number, and object that is being tracked.
IP routing is	State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.
Tracked by	Client process that is tracking the object.
First-hop interface is	Displays the first-hop interface.
Object type	Object type that is being tracked.
Poll Interval	Interval (in seconds) in which the tracking process polls the object.
Time to next poll	Period of time, in seconds, until the next polling of the object.

The following output shows that there are two objects. Object 1 has been configured with a weight of 10 “down,” and object 2 has been configured with a weight of 20 “up.” Object 1 is down (expressed as 0/10) and object 2 is up. The total weight of the tracked list is 20 with a maximum of 30 (expressed as 20/30). The “up” threshold is 20, so the list is “up.”

```
Router# show track

 Track 6
 List threshold weight
  Threshold weight is Up (20/30)
   1 change, last change 00:00:08
```

```
   object 1 Down (0/10)
   object 2 weight 20 Up (20/30)
  Threshold weight down 10 up 20
   Tracked by:
    HSRP Ethernet0/3 1
```

The following example shows information about the Boolean configuration:

```
Router# show track

 Track 3
 List boolean and
 Boolean AND is Down
  1 change, last change 00:00:08
   object 1 not Up
   object 2 Down
 Tracked by:
  HSRP Ethernet0/3 1
```

Table 312 describes the significant fields shown in the displays.

Table 312 show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Boolean AND is Down	Each object defined in the list must be in a down state.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.
Tracked by	Client process that is tracking the object; in this case, HSRP.

The following example shows information about a stub object that has been created to be tracked using Embedded Event Manager (EEM):

```
Router# show track

Track 1
  Stub-object
  State is Up
    1 change, last change 00:00:04, by Undefined
```

The following example shows information about a stub object when the **brief** keyword is used:

```
Router# show track brief

Track   Object                          Parameter        Value Last Change
1       Stub-object Undefined                            Up    00:00:12
```

The following example shows information about the line-protocol state on an interface that is being tracked and which has carrier-delay detection enabled:

```
Router# show track

Track 101
Interface Ethernet1/0 line-protocol
Line protocol is Down (carrier-delay)
1 change, last change 00:00:03
```

Table 313 describes the significant fields shown in the displays.

Table 313 show track brief Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface Ethernet1/0 line-protocol	Interface type, interface number, and object that is being tracked.
Line protocol is Down (carrier-delay)	State of the interface with the carrier-delay parameter taken into consideration.
last change	Time (in *hh:mm:ss*) since the state of a tracked object last changed.

Table 314 describes the significant fields shown in the displays.

Table 314 show track brief Field Descriptions

Field	Description
Track	Object number that is being tracked.
Object	Definition of stub object.
Parameter	Tracking parameters.
Value	State value of the object, displayed as Up or Down.
last change	Time (in *hh:mm:ss*) since the state of a tracked object last changed.

Related Commands

Command	Description
track interface	Configures an interface to be tracked and enters tracking configuration mode.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

show tunnel 6rd

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show tunnel 6rd tunnel 1

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

Table 273 describes the significant fields shown in the display.

Table 315 show tunnel 6rd Field Descriptions

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

Table 315 show tunnel 6rd Field Descriptions (continued)

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

Related Commands

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

show tunnel 6rd destination

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

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

Table 316 show tunnel 6rd destination Field Descriptions

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

Related Commands

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

show voip rtp connections

To display Real-Time Transport Protocol (RTP) named event packets, use the **show voip rtp connections** command in privileged EXEC mode.

show voip rtp connections [**detail**]

Syntax Description

detail	(Optional) Displays the called-party and calling-party numbers associated with a call.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0	This command was introduced.
12.3(7)T	The **detail** keyword was added.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
12.4(22)T	Command output was updated to show IPv6 information.

Usage Guidelines

This command displays information about RTP named event packets, such as caller ID number, IP address, and port for both the local and remote endpoints. The output from this command provides an overview of all the connections in the system, and this information can be used to narrow the criteria for debugging. The **debug voip rtp** command floods the console with voice packet information. You can use the **show voip rtp connections** command to get caller ID, remote IP address, or remote port identifiers that you can use to limit the output from the **debug voip rtp** command.

The **detail** keyword allows you to identify the phone or phones that have connected two RTP call legs to create VoIP-to-VoIP or VoIP-to-POTS hairpins. If the **detail** keyword is omitted, the output does not display calls that are connected by hairpin call routing.

Examples

Table 317 describes the significant fields shown in the examples. Each line of output under "VoIP RTP active connections" shows information for one call leg. A phone call normally consists of two call legs, one connected to the calling party and one connected to the called party. The router joins (or bridges) the two call legs to make a call. The **show voip rtp connections** command shows the RTP information for H.323 and Session Initiation Protocol (SIP) calls only; it does not directly show the POTS call legs. The information for the IP phone can be seen using the **show ephone offhook** command.

The following sample output shows an incoming H.323 call that is being directed to an IP phone attached to a Cisco CallManager Express (CME) system.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP          RemoteIP
1   21      22         16996    18174  10.4.204.37      10.4.204.24
```

```
Found 1 active RTP connections
```

The following sample output shows the same call as in the previous example, but using the **detail** keyword with the command. The sample output shows the called number (1509) and calling number (8108) on both call legs (21 and 22); the called and calling numbers are the same on both legs for a simple A-to-B call. Leg 21 is the H.323 segment of the and leg 22 is the POTS segment that goes to the IP phone.

```
Router# show voip rtp connections detail

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP          RemoteIP
1   21      22         16996    18174  10.4.204.37      10.4.204.24
  callId 21 (dir=1):called=1509 calling=8108 redirect=
     dest callId 22:called=1509 calling=8108 redirect=
   1 context 64FB3358 xmitFunc 6032E8B4
Found 1 active RTP connections
```

The following example shows the call from the previous example being transferred by extension 1509 to extension 1514. Notice that the dstCallId changed from 22 to 24, but the original call leg (21) for the transferred party is still present. This implies that H.450.2 capability was disabled for this particular call, because if H.450.2 was being used for the transfer, the transfer would have caused the incoming H.323 call leg to be replaced with a new call.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   21      24         16996    18174  10.4.204.37      10.4.204.24
Found 1 active RTP connections
```

The following example shows the detailed output for the same transfer as shown in the previous example. The original incoming call leg is still present (21) and still has the original called and calling numbers. The transferred call leg (24) shows 1509 (the transferring party) as the calling party and 1514 (the transfer destination) as the called party.

```
Router# show voip rtp connections detail

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   21      24         16996    18174  10.4.204.37      10.4.204.24
  callId 21 (dir=1):called=1509 calling=8108 redirect=
     dest callId 24:called=1514 calling=1509 redirect=
   1 context 6466E810 xmitFunc 6032E8B4
Found 1 active RTP connections
```

The following sample output shows a cross-linked call with two H.323 call legs. The first line of output shows that the CallID for the first call leg is 7 and that this call leg is associated with another call leg that has a destination CallId of 8. The next line shows that the CallID for the leg is 8 and that it is associated with another call leg that has a destination CallId of 7. This cross-linkage between CallIds 7 and 8 shows that the first call leg is related to the second call leg (and vice versa). From this you can infer that the two call legs are actually part of the same phone call.

In an active system you can expect many lines of output that you would have to sort through to see which ones have this cross-linkage relationship. The lines showing two related call legs are not necessarily listed in adjacent order.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId   dstCallId          LocalRTP     RmtRTP         LocalIP        RemoteIP
1        7           8             16586      22346      172.27.82.2      172.29.82.2
2        8           7             17010      16590      172.27.82.2      192.168.1.29
```

```
Found 2 active RTP connections
```

The following example shows RTP information with IPv6 local and remote addresses:

```
Router# show voip rtp connections

VoIP RTP active connections :
No.  CallId   dstCallId  LocalRTP  RmtRTP   LocalIP                            RemoteIP
1     11      9          17424     18282    2001:DB8:C18:1:218:FEFF:FE71:2AB6
2001:DB8:C18:1:218:FEFF:FE71:2AB6
2     12      10         18282     17424    2001:DB8:C18:1:218:FEFF:FE71:2AB6
2001:DB8:C18:1:218:FEFF:FE71:2AB6

Found 2 active RTP connections
```

Table 317 show voip rtp connections Field Descriptions

Field	Description
No.	Identifier of an RTP connection in this output.
CallId	Internal call identifier of a telephony call leg (RTP connection).
dstCallId	Internal call identifier of a VoIP call leg.
LocalRTP	RTP port of the media stream for the local entity.
RmtRTP	RTP port of the media stream for the remote entity.
LocalIP	IPv4 or IPv6 address of the media stream for the local entity.
RemoteIP	IPv4 or IPv6 address of the media stream for the remote entity.
dir	0 indicates an outgoing call. 1 indicates an incoming call.
called	Extension that received the call.
calling	Extension that made the call.
redirect	Original called number if the incoming call was forwarded.
context	Internal memory address for the control block associated with the call.
xmitFunc	Internal memory address for the transmit function to which incoming RTP packets (on the H.323 and SIP side) are sent; the address for the function that delivers the packets to the ephone.

Related Commands

Command	Description
debug voip rtp	Enables debugging for RTP named event packets.
show ephone offhook	Displays information and packet counts for phones that are currently off hook.

show vpdn session

To display session information about active Layer 2 sessions for a virtual private dialup network (VPDN), use the **show vpdn session** command in privileged EXEC mode.

show vpdn session [**l2f** | **l2tp** | **pptp**] [**all** | **packets** [**ipv6**] | **sequence** | **state** [*filter*]]

Syntax Description

l2f	(Optional) Displays information about Layer 2 Forwarding (L2F) calls only.
l2tp	(Optional) Displays information about Layer 2 Tunnel Protocol (L2TP) calls only.
pptp	(Optional) Displays information about Point-to-Point Tunnel Protocol (PPTP) calls only.
all	(Optional) Displays extensive reports about active sessions.
packets	(Optional) Displays information about packet and byte counts for sessions.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
sequence	(Optional) Displays sequence information for sessions.
state	(Optional) Displays state information for sessions.
filter	(Optional) One of the filter parameters defined in Table 318.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	This command was enhanced to display Point-to-Point Protocol over Ethernet (PPPoE) session information. The **packets** and **all** keywords were added.
12.1(2)T	This command was enhanced to display PPPoE session information on actual Ethernet interfaces.
12.2(13)T	Reports from this command were enhanced with a unique identifier that can be used to correlate a particular session with the session information retrieved from other **show** commands or **debug** command traces.
12.3(2)T	The **l2f**, **l2tp**, and **pptp** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	The **l2f** keyword was removed.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show vpdn session** command with the **all** and **l2tp all** keywords was modified to display IPv6 counter information.

Usage Guidelines

Use the **show vpdn session** command to display information about all active sessions using L2TP, L2F, and PPTP.

The output of the **show vpdn session** command displays PPPoE session information as well. PPPoE is supported on ATM permanent virtual connections (PVCs) compliant with RFC 1483 only. PPPoE is not supported on Frame Relay and any other LAN interfaces such as FDDI and Token Ring.

Reports and options for this command depend upon the configuration in which it is used. Use the command-line question mark (?) help function to display options available with the **show vpdn session** command.

Table 318 defines the filter parameters available to refine the output of the **show vpdn session** command. You may use any one of the filter parameters in place of the *filter* argument.

Table 318 Filter Parameters for the show vpdn session Command

Syntax	Description
interface serial *number*	Filters the output to display only information for sessions associated with the specified serial interface. • *number*—The serial interface number.
interface virtual-template *number*	Filters the output to display only information for sessions associated with the specified virtual template. • *number*—The virtual template number.
tunnel id *tunnel-id session-id*	Filters the output to display only information for sessions associated with the specified tunnel ID and session ID. • *tunnel-id*—The local tunnel ID. Valid values range from 1 to 65535. • *session-id*—The local session ID. Valid values range from 1 to 65535.
tunnel remote-name *remote-name local-name*	Filters the output to display only information for sessions associated with the tunnel with the specified names. • *remote-name*—The remote tunnel name. • *local-name*—The local tunnel name.
username *username*	Filters the output to display only information for sessions associated with the specified username. • *username*—The username.

The **show vpdn session** command provides reports on call activity for all active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session

L2TP Session Information Total tunnels 1 sessions 4

LocID RemID TunID Intf          Username             State    Last Chg Uniq ID
4     691   13695 Se0/0         nobody2@cisco.com        est    00:06:00  4
5     692   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  8
6     693   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  9
3     690   13695 SSS Circuit   nobody3@cisco.com        est    2d21h     3

L2F Session Information Total tunnels 1 sessions 2

 CLID   MID    Username                   Intf          State   Uniq ID
 1      2      nobody@cisco.com              SSS Circuit   open    10
 1      3      nobody@cisco.com              SSS Circuit   open    11
```

```
%No active PPTP tunnels

PPPoE Session Information Total tunnels 1 sessions 7

PPPoE Session Information
UID     SID     RemMAC          OIntf           Intf       Session
                LocMAC                          VASt       state
3       1       0030.949b.b4a0 Fa2/0            N/A        CNCT_FWDED
                0010.7b90.0840
6       2       0030.949b.b4a0 Fa2/0            Vi1.1      CNCT_PTA
                0010.7b90.0840                 UP
7       3       0030.949b.b4a0 Fa2/0            Vi1.2      CNCT_PTA
                0010.7b90.0840                 UP
8       4       0030.949b.b4a0 Fa2/0            N/A        CNCT_FWDED
                0010.7b90.0840
9       5       0030.949b.b4a0 Fa2/0            N/A        CNCT_FWDED
                0010.7b90.0840
10      6       0030.949b.b4a0 Fa2/0            N/A        CNCT_FWDED
                0010.7b90.0840
11      7       0030.949b.b4a0 Fa2/0            N/A        CNCT_FWDED
                0010.7b90.0840
```

Table 319 describes the significant fields shown in the **show vpdn session** display.

Table 319 show vpdn session Field Descriptions

Field	Description
LocID	Local identifier.
RemID	Remote identifier.
TunID	Tunnel identifier.
Intf	Interface associated with the session.
Username	User domain name.
State	Status for the individual user in the tunnel; can be one of the following states: • est • opening • open • closing • closed • waiting_for_tunnel The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
Last Chg	Time interval (in hh:mm:ss) since the last change occurred.
Uniq ID	The unique identifier used to correlate this particular session with the sessions retrieved from other **show** commands or **debug** command traces.
CLID	A number uniquely identifying the session.
MID	A number uniquely identifying this user in this tunnel.
UID	PPPoE user ID.

Table 319 show vpdn session Field Descriptions (continued)

Field	Description
SID	PPPoE session ID.
RemMAC	Remote MAC address of the host.
LocMAC	Local MAC address of the router. It is the default MAC address of the router.
OIntf	Outgoing interface.
Intf VASt	Virtual access interface number and state.
Session state	PPPoE session state.

The **show vpdn session packets** command provides reports on call activity for all the currently active sessions. The following output is from a device carrying an active PPPoE session:

```
Router# show vpdn session packets

%No active L2TP tunnels
%No active L2F tunnels

PPPoE Session Information Total tunnels 1 sessions 1
PPPoE Session Information
SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
1       202333          202337          2832652         2832716
```

Table 320 describes the significant fields shown in the **show vpdn session packets** command display.

Table 320 show vpdn session packets Field Descriptions

Field	Description
SID	Session ID for the PPPoE session.
Pkts-In	Number of packets coming into this session.
Pkts-Out	Number of packets going out of this session.
Bytes-In	Number of bytes coming into this session.
Bytes-Out	Number of bytes going out of this session.

The **show vpdn session all** command provides extensive reports on call activity for all the currently active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session all

L2TP Session Information Total tunnels 1 sessions 4

Session id 5 is up, tunnel id 13695
Call serial number is 3355500002
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:03:53
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface
```

```
    Remote session id is 692, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 8

Session id 6 is up, tunnel id 13695
Call serial number is 3355500003
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:04:22
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface
    Remote session id is 693, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 9

Session id 3 is up, tunnel id 13695
Call serial number is 3355500000
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 2d21h
    48693 Packets sent, 48692 received
    1947720 Bytes sent, 1314568 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody2@cisco.com
    Interface
    Remote session id is 690, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 3

Session id 4 is up, tunnel id 13695
Call serial number is 3355500001
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:08:40
    109 Packets sent, 3 received
    1756 Bytes sent, 54 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface Se0/0
    Remote session id is 691, remote tunnel id 58582
  UDP checksums are disabled
  IDB switching enabled
  FS cached header information:
    encap size = 36 bytes
    4500001C BDDC0000 FF11E977 0A00003E
    0A00003F 06A506A5 00080000 0202E4D6
    02B30000
  Sequencing is off
  Unique ID is 4
```

```
L2F Session Information Total tunnels 1 sessions 2
MID: 2
User:  nobody@cisco.com
Interface:
State:  open
Packets out: 53
Bytes out: 2264
Packets in: 51
Bytes in: 1274
Unique ID: 10

  Last clearing of "show vpdn" counters never
MID: 3
User:  nobody@cisco.com
Interface:
State:  open
Packets out: 53
Bytes out: 2264
Packets in: 51
Bytes in: 1274
Unique ID: 11

Last clearing of "show vpdn" counters never

%No active PPTP tunnels

PPPoE Session Information Total tunnels 1 sessions 7

PPPoE Session Information
SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
1       48696           48696           681765          1314657
2       71              73              1019            1043
3       71              73              1019            1043
4       61              62              879             1567
5       61              62              879             1567
6       55              55              791             1363
7       55              55              795             1363
```

The significant fields shown in the **show vpdn session all** command display are similar to those defined in Table 319 and Table 320.

Related Commands

Command	Description
show sss session	Displays Subscriber Service Switch session status.
show vpdn	Displays basic information about all active VPDN tunnels.
show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.
show vpdn group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information.
show vpdn history failure	Displays the content of the failure history table.
show vpdn multilink	Displays the multilink sessions authorized for all VPDN groups.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.

show vpdn tunnel

To display information about active Layer 2 tunnels for a virtual private dialup network (VPDN), use the **show vpdn tunnel** command in privileged EXEC mode.

show vpdn tunnel [**l2f** | **l2tp** | **pptp**] [**all** [*filter*] | **packets** [**ipv6**] [*filter*] | **state** [*filter*] | **summary** [*filter*] | **transport** [*filter*]]

Syntax Description

l2f	(Optional) Specifies that only information about Layer 2 Forwarding (L2F) tunnels will be displayed.
l2tp	(Optional) Specifies that only information about Layer 2 Tunnel Protocol (L2TP) tunnels will be displayed.
pptp	(Optional) Specifies that only information about Point-to-Point Tunnel Protocol (PPTP) tunnels will be displayed.
all	(Optional) Displays summary information about all active tunnels.
filter	(Optional) One of the filter parameters defined in Table 321.
packets	(Optional) Displays packet numbers and packet byte information.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
state	(Optional) Displays state information for a tunnel.
summary	(Optional) Displays a summary of tunnel information.
transport	(Optional) Displays tunnel transport information.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	The **packet**s and **all** keywords were added.
12.3(2)T	The **l2f**, **l2tp**, and **pptp** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and support was added for L2TP congestion avoidance statistics.
12.4(11)T	The **l2f** keyword was removed.
12.2(33)SB	This command's output was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show vpdn tunnel** command with the **all** and **l2tp all** keywords was modified to display IPv6 counter information.

Usage Guidelines

Use the **show vpdn tunnel** command to display detailed information about L2TP, L2F, and PPTP VPDN tunnels.

Table 321 defines the filter parameters available to refine the output of the **show vpdn tunnel** command. You may use any one of the filter parameters in place of the *filter* argument.

Table 321 Filter Parameters for the show vpdn tunnel Command

Syntax	Description
id *local-id*	Filters the output to display only information for the tunnel with the specified local ID. • *local-id*—The local tunnel ID number. Valid values range from 1 to 65535.
local-name *local-name remote-name*	Filters the output to display only information for the tunnel associated with the specified names. • *local-name*—The local tunnel name. • *remote-name*—The remote tunnel name.
remote-name *remote-name local-name*	Filters the output to display only information for the tunnel associated with the specified names. • *remote-name*—The remote tunnel name. • *local-name*—The local tunnel name.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the **show vpdn tunnel summary** command no longer displays the active PPPoE sessions. Instead, use the **show pppoe sessions** command to display the active sessions.

In Cisco IOS Release 12.2(31)SB, the **show vpdn tunnel summary** command does display the active PPPoE sessions.

Examples

The following is sample output from the **show vpdn tunnel** command for L2F and L2TP sessions:

```
Router# show vpdn tunnel

L2TP Tunnel Information (Total tunnels=1 sessions=1)
LocID RemID Remote Name   State  Remote Address  Port  Sessions
2     10    router1       est    172.21.9.13     1701  1

L2F Tunnel
 NAS CLID HGW CLID NAS Name        HGW Name        State
 9         1        nas1           HGW1            open
                    172.21.9.4      172.21.9.232

%No active PPTP tunnels
```

Table 322 describes the significant fields shown in the display.

Table 322 show vpdn tunnel Field Descriptions

Field	Description
LocID	Local tunnel identifier.
RemID	Remote tunnel identifier.
Remote Name	Hostname of the remote peer.

Table 322 show vpdn tunnel Field Descriptions (continued)

Field	Description
State	Status for the individual user in the tunnel; can be one of the following states: • est • opening • open • closing • closed • waiting_for_tunnel The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
Remote address	IP address of the remote peer.
Port	Port ID.
Sessions	Number of sessions using the tunnel.
NAS CLID	A number uniquely identifying the VPDN tunnel on the network access server (NAS).
HGW CLID	A number uniquely identifying the VPDN tunnel on the gateway.
NAS Name	Hostname and IP address of the NAS.
HGW Name	Hostname and IP address of the home gateway.

The following example shows L2TP tunnel activity, including information about the L2TP congestion avoidance:

```
Router# show vpdn tunnel l2tp all

L2TP Tunnel Information Total tunnels 1 sessions 1

Tunnel id 30597 is up, remote id is 45078, 1 active sessions
  Tunnel state is established, time since change 00:08:27
  Tunnel transport is UDP (17)
  Remote tunnel name is LAC1
    Internet Address 172.18.184.230, port 1701
  Local tunnel name is LNS1
    Internet Address 172.18.184.231, port 1701
  Tunnel domain unknown
  VPDN group for tunnel is 1
  L2TP class for tunnel is
  4 packets sent, 3 received
  194 bytes sent, 42 received
  Last clearing of "show vpdn" counters never
  Control Ns 2, Nr 4
  Local RWS 1024 (default), Remote RWS 256
  In Use Remote RWS 15
  Control channel Congestion Control is enabled
    Congestion Window size, Cwnd 3
    Slow Start threshold, Ssthresh 256
    Mode of operation is Slow Start
  Tunnel PMTU checking disabled
  Retransmission time 1, max 2 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 1
```

```
Total resends 0, ZLB ACKs sent 2
Current nosession queue check 0 of 5
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
Sessions disconnected due to lack of resources 0
Control message authentication is disabled
```

Table 323 describes the significant fields shown in the display.

Table 323 show vpdn tunnel all Field Descriptions

Field	Description
Local RWS	Size of the locally configured receive window.
Remote RWS	Size of the receive window advertised by the remote peer.
In Use RWS	Actual size of the receive window, if that value differs from the value advertised by the remote peer.
Congestion Window size, Cwnd 3	Current size of the congestion window (Cwnd).
Slow Start threshold, Ssthresh 500	Current value of the slow start threshold (Ssthresh).
Mode of operation is...	Indicates if the router is operating in Slow Start or Congestion Avoidance mode.

Related Commands

Command	Description
show vpdn	Displays basic information about all active VPDN tunnels.
show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.
show vpdn group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information.
show vpdn history failure	Displays the content of the failure history table.
show vpdn multilink	Displays the multilink sessions authorized for all VPDN groups.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.

show vrf

To display the defined Virtual Private Network (VPN) routing and forwarding (VRF) instances, use the **show vrf** command in user EXEC or privileged EXEC mode.

show vrf [**ipv4** | **ipv6**] [**interface** | **brief** | **detail** | **id** | **select** | **lock**] [*vrf-name*]

Syntax Description

ipv4	(Optional) Displays IPv4 address family-type VRF instances.
ipv6	(Optional) Displays IPv6 address family-type VRF instances.
interface	(Optional) Displays the interface associated with the specified VRF instances.
brief	(Optional) Displays brief information about the specified VRF instances.
detail	(Optional) Displays detailed information about the specified VRF instances.
id	(Optional) Displays VPN-ID information for the specified VRF instances.
select	(Optional) Displays selection information for the specified VRF instances.
lock	(Optional) Displays VPN lock information for the specified VRF instances.
vrf-name	(Optional) Name assigned to a VRF.

Command Default

If you do not specify any arguments or keywords, the command displays concise information about all configured VRFs.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. When backup paths have been created either through the Prefix Independent Convergence or Best External feature, the output of the **show vrf detail** command displays the following line: `Prefix protection with additional path enabled`
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use the **show vrf** command to display information about specified VRF instances or all VRF instances. Specify no arguments or keywords to display information on all VRF instances.

Examples

The following sample output from the **show vrf** command displays brief information about all configured VRF instances:

```
Router# show vrf

  Name                              Default RD          Protocols   Interfaces
  N1                                100:0               ipv4,ipv6
  V1                                1:1                 ipv4        Lo1
  V2                                2:2                 ipv4,ipv6   Et0/1.1
                                                                    Et0/1.2
                                                                    Et0/1.3
  V3                                3:3                 ipv4        Lo3
                                                                    Et0/1.4
```

Table 324 describes the significant fields shown in the display.

Table 324 show vrf Field Descriptions

Field	Description
Name	Name of the VRF instance.
Default RD	The default route distinguisher (RD) for the specified VRF instances.
Protocols	The address family protocol type for the specified VRF instance.
Interfaces	The network interface associated with the VRF instance.

The following sample output from the **show vrf** command with the **detail** keyword displays information for a VRF named cisco:.

```
Router# show vrf detail

VRF cisco1; default RD 100:1; default VPNID <not set>
  Interfaces:
    Ethernet0/0                  Loopback10
Address family ipv4 (Table ID = 0x1):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
Address family ipv6 (Table ID = 0xE000001):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

Table 325 describes the significant fields shown in the display.

Table 325 show vrf detail Field Descriptions

Field	Description
default RD 100:1	The RD given to this VRF.
Interfaces:	Interfaces to which the VRF is attached.
Export VPN route-target communities RT:100:1	Route-target VPN extended communities to be exported.
Import VPN route-target communities RT:100:1	Route-target VPN extended communities to be imported.

The following example displays output from the **show vrf detail** command when backup paths have been created either through the Prefix Independent Convergence or Best External feature. The output of the **show vrf detail** command displays the following line:

```
Prefix protection with additional path enabled
```

```
Router# show vrf detail

VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
  Interfaces:
    Et1/1
Address family ipv4 (Table ID = 1 (0x1)):
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
  Prefix protection with additional path enabled
Address family ipv6 not active.
```

The following sample output from the **show vrf lock** command displays VPN lock information:

```
Router# show vrf lock

VRF Name: Mgmt-intf; VRF id = 4085 (0xFF5)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :108
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
VRF Name: vpn1; VRF id = 1 (0x1)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :100
```

```
Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
Caller PC tracebacks:
Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
```

Related Commands

Command	Description
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.
vrf forwarding	Associates a VRF instance with an interface or subinterface.

shutdown (gateway)

To shut down all VoIP call service on a gateway, use the **shutdown** command in voice service configuration mode. To enable VoIP call service, use the **no** form of this command.

shutdown [**forced**]

no shutdown

Syntax Description

forced	(Optional) Forces the gateway to immediately terminate all in-progress calls.

Command Default

Call service is enabled

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example shows VoIP call service being shut down on a Cisco gateway:

```
voice service voip
shutdown
```

The following example shows VoIP call service being enabled on a Cisco gateway:

```
voice service voip
no shutdown
```

Related Commands

Command	Description
shutdown (gatekeeper)	Disables the gatekeeper.

single-connection

To enable all TACACS packets to be sent to the same server using a single TCP connection, use the **single-connection** command in TACACS+ server configuration mode. To disable this feature, use the **no** form of this command.

single-connection

no single-connection

Syntax Description

This command has no arguments or keywords.

Command Default

TACACS packets are not sent on a single TCP connection.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

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

Usage Guidelines

Use the **single-connection** command to multiplex all TACACS packets to the same server over a single TCP connection.

Examples

The following example shows how to multiplex all TACACS packets over a single TCP connection to the TACACS server:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# single-connection
```

Related Commands

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

sip address

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

sip address *ipv6-address*

no sip address *ipv6-address*

Syntax Description

ipv6-address	An IPv6 address. The *ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No default behavior or values

Command Modes

DHCP for IPv6 pool configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

sip domain-name

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

sip domain-name *domain-name*

no sip domain-name *domain-name*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

DHCP for IPv6 pool configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

sip-server

To configure a network address for the Session Initiation Protocol (SIP) server interface, use the **sip-server** command in SIP user-agent configuration mode. To remove a network address configured for SIP, use the **no** form of this command.

sip-server {**dns:**[*host-name*] | **ipv4:***ipv4-address* | **ipv6:**[*ipv6-address*][**:***port-num*]}

no sip-server

Syntax Description

dns:	Sets the global SIP server interface to a Domain Name System (DNS) hostname. If you do not specify a hostname, the default DNS defined by the **ip name-server** command is used.
host-name	(Optional) Valid DNS hostname in the following format: name.gateway.xyz.
ipv4:*ipv4-address*	Sets the global SIP server interface to an IPv4 address. A valid IPv4 address takes the following format: xxx.xxx.xxx.xxx.
ipv6:[*ipv6-address*]	Sets the global SIP server interface to an IPv6 address. You must enter brackets around the IPv6 address.
:*port-num*	(Optional) Port number for the SIP server.

Command Default

No network address is configured.

Command Modes

SIP user-agent configuration (conf-serv-sip)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

If you use this command, you can also use the **session target sip-server** command on each dial peer instead of repeatedly entering the SIP server interface address for each dial peer. Configuring a SIP server as a session target is useful if a Cisco SIP proxy server (SPS) is present in the network. With an SPS, you can configure the SIP server option and have the interested dial peers use the SPS by default.

To reset this command to a null value, use the **default** command.

To configure an IPv6 address, the user must enter brackets [ ] around the IPv6 address.

Examples

The following example, beginning in global configuration mode, sets the global SIP server interface to the DNS hostname "3660-2.sip.com." If you also use the **session target sip server** command, you need not set the DNS hostname for each individual dial peer.

```
sip-ua
 sip-server dns:3660-2.sip.com

dial-peer voice 29 voip
 session target sip-server
```

The following example sets the global SIP server interface to an IPv4 address:

```
sip-ua
 sip-server ipv4:10.0.2.254
```

The following example sets the global SIP server interface to an IPv6 address. Note that brackets were entered around the IPv6 address:

```
sip-ua
 sip-server ipv6:[2001:0DB8:0:0:8:800:200C:417A]
```

Related Commands

Command	Description
default	Enables a default aggregation cache.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
session target (VoIP dial peer)	Specifies a network-specific address for a dial peer.
session target sip-server	Instructs the dial peer session target to use the global SIP server.
sip-ua	Enters SIP user-agent configuration mode in order to configure the SIP user agent.

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*]

no snmp-server community *string*

Syntax Description

string	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
view	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community.
view-name	(Optional) Name of a previously defined view.
ro	(Optional) Specifies read-only access. Authorized management stations can retrieve only MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.
ipv6	(Optional) Specifies an IPv6 named access list.
nacl	(Optional) IPv6 named access list.
access-list-number	(Optional) Integer from 1 to 99 that specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent. Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers that are allowed to use the community string to gain access to the SNMP agent.

Command Default

An SNMP community string permits read-only access to all objects.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.3(2)T	The access list values were enhanced to support the expanded range of standard access list values and to support named standard access lists.
12.0(27)S	The **ipv6** *nacl* keyword and argument pair was added to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.3(14)T	The **ipv6** *nacl* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
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(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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 Aggregation Series Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SRE	This command was modified. The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, is changed. The **snmp-server community** command has to be manually configured.
15.1(0)M	This command was modified. The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, is changed. The **snmp-server community** command has to be manually configured.

Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

The first **snmp-server** command that you enter enables all versions of SNMP.

To configure SNMP community strings for the MPLS LDP MIB, use the **snmp-server community** command on the host network management station (NMS).

Note In Cisco IOS Release 12.0(3) to 12.2(33)SRD, if a community string was not defined using the **snmp-server community** command prior to using the **snmp-server host** command, the default form of the **snmp-server community** command was automatically inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** was same as specified in the **snmp-server host** command. However, in Cisco IOS Release 12.2(33)SRE and later releases, you have to manually configure the **snmp-server community** command.

The **snmp-server community** command can be used to specify only an IPv6 named access list, only an IPv4 access list, or both. For you to configure both IPv4 and IPv6 access lists, the IPv6 access list must appear first in the command statement.

Note The @ symbol is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using community@VLAN_ID (for example, public@100) where 100 is the VLAN number. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

Examples

The following example shows how to set the read/write community string to newstring:

```
Router(config)# snmp-server community newstring rw
```

The following example shows how to allow read-only access for all objects to members of the standard named access list lmnop that specify the comaccess community string. No other SNMP managers have access to any objects.

```
Router(config)# snmp-server community comaccess ro lmnop
```

The following example shows how to assign the string comaccess to SNMP, allow read-only access, and specify that IP access list 4 can use the community string:

```
Router(config)# snmp-server community comaccess ro 4
```

The following example shows how to assign the string manager to SNMP and allow read-write access to the objects in the restricted view:

```
Router(config)# snmp-server community manager view restricted rw
```

The following example shows how to remove the community comaccess:

```
Router(config)# no snmp-server community comaccess
```

The following example shows how to disable all versions of SNMP:

```
Router(config)# no snmp-server
```

The following example shows how to configure an IPv6 access list named list1 and links an SNMP community string with this access list:

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# exit
Router(config)# snmp-server community comaccess rw ipv6 list1
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
show snmp community	Displays SNMP community access strings.
snmp-server enable traps	Enables the router to send SNMP notification messages to a designated network management workstation.
snmp-server host	Specifies the targeted recipient of an SNMP notification operation.
snmp-server view	Creates or updates a view entry.

snmp-server engineID remote

To specify the Simple Network Management Protocol (SNMP) engine ID of a remote SNMP device, use the **snmp-server engineID remote** command in global configuration mode. To remove a specified SNMP engine ID from the configuration, use the **no** form of this command.

snmp-server engineID remote {*ipv4-ip-address* | *ipv6 address*}[**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*

no snmp-server engineID remote {*ipv4-ip-address* | *ipv6 address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*

Syntax Description

ipv4-ip-address | *ipv6-address*	IPv4 or IPv6 address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a User Datagram Protocol (UDP) port of the host to use.
udp-port-number	(Optional) Socket number on the remote device that contains the remote copy of SNMP. The default is 161.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
engineid-string	String of a maximum of 24 characters that identifies the engine ID.

Command Default

The default is UDP port 161.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(2)T	The **vrf** keyword and *vrf-name* argument were added.
12.0(27)S	Support for configuring an IPv6 notification server was added.
12.3(14)T	Support for configuring an IPv6 notification server was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Specifying the entire 24-character engine ID if it contains trailing zeros is not required. Specify only the portion of the engine ID up to where the trailing zeros start. For example, to configure an engine ID of 123400000000000000000000, specify the value 1234 as the *engineid-string* argument.

A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Examples

The following example specifies the SNMP engine ID and configures the VRF name traps-vrf for SNMP communications with the remote device at 172.16.20.3:

```
Router(config)# snmp-server engineID remote 172.16.20.3 vrf traps-vrf
80000009030000B064EFE100
```

Related Commands

Command	Description
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
snmp-server host	Specifies the recipient (SNMP manager) of an SNMP trap notification.

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number* | *acl-name*]]

no snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

Syntax Description

group-name	Name of the group.
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
context-name	(Optional) Context name.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
read-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.
notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.

notify-view	(Optional) String of a maximum of 64 characters that is the name of the view. By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user). Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.
acl-number	(Optional) The *acl-number* argument is an integer from 1 to 99 that identifies a previously configured standard access list.
acl-name	(Optional) The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.

Command Default

No SNMP server groups are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.(3)T	This command was introduced.
12.0(23)S	The **context** *context-name* keyword and argument pair was added.
12.3(2)T	The **context** *context-name* keyword and argument pair was integrated into Cisco IOS Release 12.3(2)T, and support for standard named access lists (acl-name) was added.
12.0(27)S	The **ipv6** *named-access-list* keyword and argument pair was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	The **ipv6** *named-access-list* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

Configuring Notify Views

The *notify-view* option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.
- Modifying the group's notify view will affect all users associated with that group.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in the order specified:

1. **snmp-server user**—Configures an SNMP user.
2. **snmp-server group**—Configures an SNMP group, without adding a notify view.
3. **snmp-server host**—Autogenerates the notify view by specifying the recipient of a trap operation.

SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

Use this command with the **context** *context-name* keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

Examples

Create an SNMP Group

The following example shows how to create the SNMP server group "public," allowing read-only access for all objects to members of the standard named access list "lmnop":

```
Router(config)# snmp-server group public v2c access lmnop
```

Remove an SNMP Server Group

The following example shows how to remove the SNMP server group "public" from the configuration:

```
Router(config)# no snmp-server group public v2c
```

Associate an SNMP Server Group with Specified Views

The following example shows SNMP context "A" associated with the views in SNMPv2c group "GROUP1":

```
Router(config)# snmp-server context A
Router(config)# snmp mib community commA
Router(config)# snmp mib community-map commA context A target-list commAVpn
Router(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

Related Commands

Command	Description
show snmp group	Displays the names of groups on the router and the security model, the status of the different views, and the storage type of each group.
snmp mib community-map	Associates a SNMP community with an SNMP context, engine ID, security name, or VPN target list.
snmp-server host	Specifies the recipient of a SNMP notification operation.
snmp-server user	Configures a new user to a SNMP group.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server host {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

no snmp-server host {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches

snmp-server host *ip-address* {*community-string* | {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string* | **vrf** *vrf-name* {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string*}} [*notification-type*]

no snmp-server host *ip-address* {*community-string* | {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string* | **vrf** *vrf-name* {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}} *community-string*}} [*notification-type*]

Command Syntax on Cisco 7600 Series Router

snmp-server host *ip-address* {*community-string* | {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* | **vrf** *vrf-name* {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string*}} [*notification-type*]

no snmp-server host *ip-address* {*community-string* | {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* | **vrf** *vrf-name* {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string*}} [*notification-type*]

Syntax Description

hostname	Name of the host. The SNMP notification host is typically a network management station (NMS) or SNMP manager. This host is the recipient of the SNMP traps or informs.
ip-address	IPv4 address or IPv6 address of the SNMP notification host.
vrf	(Optional) Specifies that a Virtual Private Network (VPN) routing and forwarding (VRF) instance should be used to send SNMP notifications. • In Cisco IOS Release 12.2(54)SE, the **vrf** keyword is required.
vrf-name	(Optional) VPN VRF instance used to send SNMP notifications. • In Cisco IOS Release 12.2(54)SE, the *vrf-name* argument is required.
informs	(Optional) Specifies that notifications should be sent as informs. • In Cisco IOS Release 12.2(54)SE, the **informs** keyword is required.

traps	(Optional) Specifies that notifications should be sent as traps. This is the default. • In Cisco IOS Release 12.2(54)SE, the **traps** keyword is required.
version	(Optional) Specifies the version of the SNMP that is used to send the traps or informs. The default is 1. • In Cisco IOS Release 12.2(54)SE, the **version** keyword is required and the **priv** keyword is not supported. If you use the **version** keyword, one of the following keywords must be specified: • **1**—SNMPv1. • **2c**—SNMPv2C. • **3**—SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**. One of the following three optional security level keywords can follow the **3** keyword: – **auth**—Enables message digest algorithm 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. – **noauth**—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. – **priv**—Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	Password-like community string sent with the notification operation. **Note** You can set this string using the **snmp-server host** command by itself, but Cisco recommends that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command. **Note** The "at" sign (@) is used for delimiting the context information.
udp-port	(Optional) Specifies that SNMP traps or informs are to be sent to an NMS host. • In Cisco IOS Release 12.2(54)SE, the **udp-port** keyword is not supported.
port	(Optional) User Datagram Protocol (UDP) port number of the NMS host. The default is 162. • In Cisco IOS Release 12.2(54)SE, the *port* argument is not supported.
notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. See the "Notification-Type Keywords" section on page 2218 in the "Usage Guidelines" section for more information about the keywords available.

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
Cisco IOS Release 12 Mainline/T Train	
12.0(3)T	• The **version 3** [**auth** | **noauth** | **priv**] syntax was added as part of the SNMPv3 Support feature. • The **hsrp** notification-type keyword was added. • The **voice** notification-type keyword was added.
12.1(3)T	The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	• The **vrf** *vrf-name* keyword and argument combination was added. • The **ipmobile** notification-type keyword was added. • Support for the **vsimaster** notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.
12.2(4)T	• The **pim** notification-type keyword was added. • The **ipsec** notification-type keyword was added.
12.2(8)T	• The **mpls-traffic-eng** notification-type keyword was added. • The **director** notification-type keyword was added.
12.2(13)T	• The **srp** notification-type keyword was added. • The **mpls-ldp** notification-type keyword was added.
12.3(2)T	• The **flash** notification-type keyword was added. • The **l2tun-session** notification-type keyword was added.
12.3(4)T	• The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added. • The **ospf** notification-type keyword was added.
12.3(8)T	The **iplocalpool** notification-type keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	The **vrrp** keyword was added.
12.3(14)T	• Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **eigrp** notification-type keyword was added.
12.4(20)T	The **license** notification-type keyword was added.
15.0(1)M	• The **nhrp** notification-type keyword was added. • The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, was changed. The **snmp-server community** command must be manually configured.
Cisco IOS Release 12.0S	
12.0(17)ST	The **mpls-traffic-eng** notification-type keyword was added.
12.0(21)ST	The **mpls-ldp** notification-type keyword was added.

Release	Modification
12.0(22)S	• All features in Cisco IOS Release 12.0ST were integrated into Cisco IOS Release 12.0(22)S. • The **mpls-vpn** notification-type keyword was added.
12.0(23)S	The **l2tun-session** notification-type keyword was added.
12.0(26)S	The **memory** notification-type keyword was added.
12.0(27)S	• Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **vrf** *vrf-name* keyword and argument combination was added to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	The **l2tun-pseudowire-status** notification-type keyword was added.
Release 12.2S	
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(25)S	• The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added.
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(31)SB2	The **cef** notification-type keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI5	• The **dhcp-snooping** notification-type keyword was added. • The **errdisable** notification-type keyword was added.
12.2(54)SE	This command was modified. See the "Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches" section on page 2213 for the command syntax for these switches.
12.2(33)SXJ	This command was integrated into Cisco IOS Release 12.2(33)SXJ. The **public storm-control** notification-type keyword was added.
12.2(50)SY	This command integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS Release 15S	
15.0(1)S	This command was modified. The **flowmon** notification-type keyword was added.
Cisco IOS XE	
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Note If a community string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** will be the same as that specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enable** command. Some notification types are always enabled, and others are enabled by a different command. For example, the **linkUpDown** notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

The availability of a notification-type options depends on the router type and the Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific virtual routing and forwarding (VRF) VPN. The VRF defines a VPN membership of a user so that data is stored using the VPN.

In the case of the NMS sending the query having a correct SNMP community but that does not have a read or a write view, the SNMP agent returns the following error values:

- For a get or a getnext query, returns GEN_ERROR for SNMPv1 and AUTHORIZATION_ERROR for SNMPv2C.
- For a set query, returns NO_ACCESS_ERROR.

Notification-Type Keywords

The notification type can be one or more of the following keywords:

Note The available notification types differ based on the platform and Cisco IOS release. For a complete list of available notification types, use the question mark (?) online help function.

- **aaa server**—Sends SNMP authentication, authorization, and accounting (AAA) traps.
- **adslline**—Sends Asymmetric Digital Subscriber Line (ADSL) LINE-MIB traps.
- **atm**—Sends ATM notifications.
- **authenticate-fail**—Sends an SNMP 802.11 Authentication Fail trap.
- **auth-framework**—Sends SNMP CISCO-AUTH-FRAMEWORK-MIB notifications.
- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
- **bridge**—Sends SNMP STP Bridge MIB notifications.
- **bstun**—Sends Block Serial Tunneling (bstun) event notifications.
- **bulkstat**—Sends Data-Collection-MIB notifications.
- **c6kxbar**—Sends SNMP crossbar notifications.
- **callhome**—Sends Call Home MIB notifications.
- **calltracker**—Sends Call Tracker call-start/call-end notifications.
- **casa**—Sends Cisco Appliances Services Architecture (CASA) event notifications.
- **ccme**—Sends SNMP Cisco netManager Event (CCME) traps.
- **cef**—Sends notifications related to Cisco Express Forwarding.
- **chassis**—Sends SNMP chassis notifications.
- **cnpd**—Sends Cisco network-based application recognition (NBAR) Protocol Discovery (CNPD) traps.
- **config**—Sends configuration change notifications.
- **config-copy**—Sends SNMP config-copy notifications.
- **config-ctid**—Sends SNMP config-ctid notifications.
- **cpu**—Sends CPU-related notifications.
- **csg**—Sends SNMP Content Services Gateway (CSG) notifications.
- **deauthenticate**—Sends an SNMP 802.11 Deauthentication trap.
- **dhcp-snooping**—Sends Dynamic Host Configuration Protocol (DHCP) snooping MIB notifications.
- **director**—Sends notifications related to DistributedDirector.
- **disassociate**—Sends an SNMP 802.11 Disassociation trap.
- **dlsw**—Sends data-link switching (DLSW) notifications.
- **dnis**—Sends SNMP Dialed Number Identification Service (DNIS) traps.
- **dot1x**—Sends 802.1X notifications.
- **dot11-mibs**—Sends dot11 traps.
- **dot11-qos**—Sends SNMP 802.11 QoS Change trap.

- **ds1**—Sends SNMP digital signaling 1 (DS1) notifications.
- **ds1-loopback**—Sends ds1-loopback traps.
- **dspu**—Sends downstream physical unit (DSPU) notifications.
- **eigrp**—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.
- **energywise**—Sends SNMP energywise notifications.
- **entity**—Sends Entity MIB modification notifications.
- **entity-diag**—Sends SNMP entity diagnostic MIB notifications.
- **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
- **errdisable**—Sends error disable notifications.
- **ethernet-cfm**—Sends SNMP Ethernet Connectivity Fault Management (CFM) notifications.
- **event-manager**—Sends SNMP Embedded Event Manager notifications.
- **firewall**—Sends SNMP Firewall traps.
- **flash**—Sends flash media insertion and removal notifications.
- **flexlinks**—Sends FLEX links notifications.
- **flowmon**—Sends flow monitoring notifications.
- **frame-relay**—Sends Frame Relay notifications.
- **fru-ctrl**—Sends entity field-replaceable unit (FRU) control notifications.
- **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
- **icsudsu**—Sends SNMP ICSUDSU traps.
- **iplocalpool**—Sends IP local pool notifications.
- **ipmobile**—Sends Mobile IP notifications.
- **ipmulticast**—Sends IP multicast notifications.
- **ipsec**—Sends IP Security (IPsec) notifications.
- **isakmp**—Sends SNMP ISAKMP notifications.
- **isdn**—Sends ISDN notifications.
- **l2tc**—Sends SNMP L2 tunnel configuration notifications.
- **l2tun-pseudowire-status**—Sends pseudowire state change notifications.
- **l2tun-session**—Sends Layer 2 tunneling session notifications.
- **license**—Sends licensing notifications as traps or informs.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
- **mac-notification**—Sends SNMP MAC notifications.
- **memory**—Sends memory pool and memory buffer pool notifications.
- **module**—Sends SNMP module notifications.
- **module-auto-shutdown**—Sends SNMP module autoshutdown MIB notifications.
- **mpls-fast-reroute**—Sends SNMP Multiprotocol Label Switching (MPLS) traffic engineering fast reroute notifications.

- **mpls-ldp**—Sends MPLS Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.
- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **msdp**—Sends SNMP Multicast Source Discovery Protocol (MSDP) notifications.
- **mvpn**—Sends multicast VPN notifications.
- **nhrp**—Sends Next Hop Resolution Protocol (NHRP) notifications.
- **ospf**—Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) notifications.
- **port-security**—Sends SNMP port-security notifications.
- **power-ethernet**—Sends SNMP power Ethernet notifications.
- **public storm-control**—Sends SNMP public storm-control notifications.
- **pw-vc**—Sends SNMP pseudowire virtual circuit (VC) notifications.
- **repeater**—Sends standard repeater (hub) notifications.
- **resource-policy**—Sends CISCO-ERM-MIB notifications.
- **rf**—Sends SNMP RF MIB notifications.
- **rogue-ap**—Sends an SNMP 802.11 Rogue AP trap.
- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Response Time Reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **slb**—Sends SNMP server load balancer (SLB) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.

  Note To enable RFC 2233-compliant link up/down notifications, you should use the **snmp server link trap** command.

- **sonet**—Sends SNMP SONET notifications.
- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **stpx**—Sends SNMP STPX MIB notifications.
- **srst**—Sends SNMP Survivable Remote Site Telephony (SRST) traps.
- **stun**—Sends serial tunnel (STUN) notifications.
- **switch-over**—Sends an SNMP 802.11 Standby Switch-over trap.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.

- **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.
- **udp-port**—Sends the notification host's UDP port number.
- **vlan-mac-limit**—Sends SNMP L2 control VLAN MAC limit notifications.
- **vlancreate**—Sends SNMP VLAN created notifications.
- **vlandelete**—Sends SNMP VLAN deleted notifications.
- **voice**—Sends SNMP voice traps.
- **vrrp**—Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vsimaster**—Sends Virtual Switch Interface (VSI) Master notifications.
- **vswitch**—Sends SNMP virtual switch notifications.
- **vtp**—Sends SNMP VLAN Trunking Protocol (VTP) notifications.
- **wlan-wep**—Sends an SNMP 802.11 Wireless LAN (WLAN) Wired Equivalent Privacy (WEP) trap.
- **x25**—Sends X.25 event notifications.
- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) traps.

SNMP-Related Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no embedded spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an embedded space and a hyphen).

This syntax difference is necessary to ensure that the CLI interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. Table 326 maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 326 SNMP-server enable traps Commands and Corresponding Notification Keywords

snmp-server enable traps Command	snmp-server host Command Keyword
snmp-server enable traps l2tun session	**l2tun-session**
snmp-server enable traps mpls ldp	**mpls-ldp**
snmp-server enable traps mpls traffic-eng[1]	**mpls-traffic-eng**
snmp-server enable traps mpls vpn	**mpls-vpn**

1. *See the Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 192.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

Note The "at" sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using *community@VLAN-ID* (for example, public@100), where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a specified host named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 192.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 192.30.2.160 public snmp envmon
```

The following example shows how to enable the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host. The community string is defined as public.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com public isdn
```

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example shows how to send all SNMP notifications to example.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host example.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public vrrp
```

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 192.40.3.130 informs version 2c public cef
```

The following example shows how to enable all NHRP traps, and how to send all NHRP traps to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 192.40.3.130 traps version 2c public nhrp
```

Related Commands

Command	Description
show snmp host	Displays recipient details configured for SNMP notifications.
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server enable traps nhrp	Enables SNMP notifications (traps) for NHRP.
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP trap that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
test snmp trap storm-control event-rev1	Tests SNMP storm-control traps.