

# show bgp ipv6 neighbors

To display information about IPv6 Border Gateway Protocol (BGP) connections to neighbors, use the **show bgp ipv6 neighbors** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} neighbors [ipv6-address] [received-routes | routes |
flap-statistics | advertised-routes | paths regular-expression | dampened-routes]
```

Syntax Description		
<b>unicast</b>		Specifies IPv6 unicast address prefixes.
<b>multicast</b>		Specifies IPv6 multicast address prefixes.
<i>ipv6-address</i>		(Optional) Address of the IPv6 BGP-speaking neighbor. If you omit this argument, all IPv6 neighbors are displayed.  This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<b>received-routes</b>		(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
<b>routes</b>		(Optional) Displays all routes received and accepted. This is a subset of the output from the <b>received-routes</b> keyword.
<b>flap-statistics</b>		(Optional) Displays flap statistics for the routes learned from the neighbor.
<b>advertised-routes</b>		(Optional) Displays all the routes the networking device advertised to the neighbor.
<b>paths</b> <i>regular-expression</i>		(Optional) Regular expression used to match the paths received.
<b>dampened-routes</b>		(Optional) Displays the dampened routes to the neighbor at the IP address specified.

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	IPv6 capability information was added to the display.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.3(2)T	The <b>unicast</b> keyword was added.
	12.0(26)S	The <b>unicast</b> and <b>multicast</b> keywords were added.
	12.3(4)T	The <b>multicast</b> 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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

**Usage Guidelines**

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

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

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

**Examples**

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

**Note**

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

```
Router# show bgp ipv6 unicast neighbors

BGP neighbor is 3FFE:700:20:1::11, remote AS 65003, external link
Member of peer-group 6BONE for session parameters
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv6 Unicast: advertised and received
Received 31306 messages, 20 notifications, 0 in queue
Sent 14298 messages, 1 notifications, 0 in queue
Default minimum time between advertisement runs is 30 seconds

For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  6BONE peer-group member
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes

Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x1A0D543C):
Timer           Starts    Wakeups      Next
Retrans         1218         5           0x0
TimeWait        0             0           0x0
```

```

AckHold          3327          3051          0x0
SendWnd          0              0              0x0
KeepAlive        0              0              0x0
GiveUp           0              0              0x0
PmtuAger         0              0              0x0
DeadWait         0              0              0x0

iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354  sndwnd: 15531
irs:  821333727  rcvnxt: 821591465  rcvwnd: 15547  delrcvwnd: 837

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle

```

```

Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128

```

The following is sample output from the **show bgp ipv6 neighbors** command when the router is configured to allow IPv6 traffic to be transported across an IPv4 Multiprotocol Label Switching (MPLS) network (Cisco 6PE) without any software or hardware upgrade in the IPv4 core infrastructure. A new neighbor capability is added to show that an MPLS label is assigned for each IPv6 address prefix to be advertised. 6PE uses multiprotocol BGP to provide the reachability information for the 6PE routers across the IPv4 network so that the neighbor addresses are IPv4.

```
Router# show bgp ipv6 unicast neighbors
```

```

BGP neighbor is 10.11.11.1, remote AS 65000, internal link
BGP version 4, remote router ID 10.11.11.1
BGP state = Established, up for 04:00:53
Last read 00:00:02, hold time is 15, keepalive interval is 5 seconds
Configured hold time is 15, keepalive interval is 10 seconds
Neighbor capabilities:
  Route refresh: advertised and received(old & new)
  Address family IPv6 Unicast: advertised and received
  ipv6 MPLS Label capability: advertised and received
Received 67068 messages, 1 notifications, 0 in queue
Sent 67110 messages, 16 notifications, 0 in queue
Default minimum time between advertisement runs is 5 seconds

For address family: IPv6 Unicast
BGP table version 91, neighbor version 91
Index 1, Offset 0, Mask 0x2
Route refresh request: received 0, sent 0
Sending Prefix & Label
4 accepted prefixes consume 288 bytes
Prefix advertised 90, suppressed 0, withdrawn 2
Number of NLRIs in the update sent: max 3, min 0

Connections established 26; dropped 25
Last reset 04:01:20, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.10.10.1, Local port: 179
Foreign host: 10.11.11.1, Foreign port: 11003

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x1429F084):
Timer           Starts      Wakeups      Next
Retrans         2971         77           0x0
TimeWait        0            0            0x0
AckHold         2894        1503         0x0
SendWnd         0            0            0x0

```

## show bgp ipv6 neighbors

```

KeepAlive          0          0          0x0
GiveUp             0          0          0x0
PmtuAger          0          0          0x0
DeadWait          0          0          0x0

```

```

iss: 803218558  snduna: 803273755  sndnxt: 803273755  sndwnd: 16289
irs: 4123967590  rcvnxt: 4124022787  rcvwnd: 16289  delrcvwnd: 95

```

```

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 32 ms, maxRTT: 408 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

```

Datagrams (max data segment is 536 bytes):

```

Rcvd: 4531 (out of order: 0), with data: 2895, total data bytes: 55215
Sent: 4577 (retransmit: 77, fastretransmit: 0), with data: 2894, total data
bytes: 55215

```

Table 119 describes the significant fields shown in the display.

**Table 119** show bgp ipv6 neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.
remote AS	Autonomous system of the neighbor.
internal link	Indicates that this peer is an interior Border Gateway Protocol (iBGP) peer.
BGP version	BGP version being used to communicate with the remote router; the router ID (an IP address) of the neighbor is also specified.
remote router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
BGP state	Internal state of this BGP connection.
up for	Amount of time that the underlying TCP connection has been in existence.
Last read	Time that BGP last read a message from this neighbor.
hold time	Maximum amount of time that can elapse between messages from the peer.
keepalive interval	Time period between sending keepalive packets, which help ensure that the TCP connection is up.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor.
Route refresh	Indicates that the neighbor supports dynamic soft reset using the route refresh capability.
Address family IPv6 Unicast	Indicates that BGP peers are exchanging IPv6 reachability information.
ipv6 MPLS Label capability	Indicates that MPLS labels are being assigned to IPv6 address prefixes.
Received notifications	Number of total BGP messages received from this peer, including keepalives.
Sent notifications	Number of error messages received from the peer.
Received notifications	Total number of BGP messages that have been sent to this peer, including keepalives.
Sent notifications	Number of error messages the router has sent to this peer.

**Table 119** *show bgp ipv6 neighbors Field Descriptions (continued)*

Field	Description
advertisement runs	Value of the minimum advertisement interval.
For address family	Address family to which the following fields refer.
BGP table version	Indicates that the neighbor has been updated with this version of the primary BGP routing table.
neighbor version	Number used by the software to track the prefixes that have been sent and those that must be sent to this neighbor.
Route refresh request	Number of route refresh requests sent and received from this neighbor.
Community attribute (not shown in sample output)	Appears if the <b>neighbor send-community</b> command is configured for this neighbor.
Inbound path policy (not shown in sample output)	Indicates whether an inbound filter list or route map is configured.
Outbound path policy (not shown in sample output)	Indicates whether an outbound filter list, route map, or unsuppress map is configured.
bgp-in (not shown in sample output)	Name of the inbound update prefix filter list for the IPv6 unicast address family.
aggregate (not shown in sample output)	Name of the outbound update prefix filter list for the IPv6 unicast address family.
uni-out (not shown in sample output)	Name of the outbound route map for the IPv6 unicast address family.
accepted prefixes	Number of prefixes accepted.
Prefix advertised	Number of prefixes advertised.
suppressed	Number of prefixes suppressed.
withdrawn	Number of prefixes withdrawn.
history paths (not shown in sample output)	Number of path entries held to remember history.
Connections established	Number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other.
dropped	Number of times that a good connection has failed or been taken down.
Last reset	Elapsed time (in hours:minutes:seconds) since this peering session was last reset.
Connection state	State of the BGP peer.
unread input bytes	Number of bytes of packets still to be processed.
Local host, Local port	Peering address of the local router, plus the port.
Foreign host, Foreign port	Peering address of the neighbor.
Event Timers	Table that displays the number of starts and wakeups for each timer.

**Table 119** show bgp ipv6 neighbors Field Descriptions (continued)

Field	Description
iss	Initial send sequence number.
snduna	Last send sequence number for which the local host sent but has not received an acknowledgment.
sndnxt	Sequence number the local host will send next.
sndwnd	TCP window size of the remote host.
irs	Initial receive sequence number.
rcvnxt	Last receive sequence number the local host has acknowledged.
rcvwnd	TCP window size of the local host.
delrcvwnd	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT	A calculated smoothed round-trip timeout (in milliseconds).
RTTO	Round-trip timeout (in milliseconds).
RTV	Variance of the round-trip time (in milliseconds).
KRTT	New round-trip timeout (in milliseconds) using the Karn algorithm. This field separately tracks the round-trip time of packets that have been re-sent.
minRTT	Smallest recorded round-trip timeout (in milliseconds) with hard wire value used for calculation.
maxRTT	Largest recorded round-trip timeout (in milliseconds).
ACK hold	Time (in milliseconds) the local host will delay an acknowledgment in order to “piggyback” data on it.
Flags	IP precedence of the BGP packets.
Datagrams: Rcvd	Number of update packets received from neighbor.
with data	Number of update packets received with data.
total data bytes	Total number of bytes of data.
Sent	Number of update packets sent.
with data	Number of update packets with data sent.
total data bytes	Total number of data bytes.

The following is sample output from the **show bgp ipv6 neighbors** command with the **advertised-routes** keyword:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes

BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11      0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2        0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2        0 3748 4697 i
```

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

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes

BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11      0 293 3425 2500 i
* 2001:208::/35    3FFE:700:20:1::11      0 293 7610 i
* 2001:218::/35    3FFE:700:20:1::11      0 293 3425 4697 i
* 2001:230::/35    3FFE:700:20:1::11      0 293 1275 3748 i
```

Table 120 describes the significant fields shown in the display.

**Table 120** *show bgp ipv6 neighbors advertised-routes and routes Field Descriptions*

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> <li>s—The table entry is suppressed.</li> <li>d—The table entry is dampened.</li> <li>h—The table entry is history.</li> <li>*—The table entry is valid.</li> <li>&gt;—The table entry is the best entry to use for that network.</li> <li>i—The table entry was learned via an internal BGP session.</li> </ul>
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> <li>i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a <b>network</b> router configuration command.</li> <li>e—Entry originated from the Exterior Gateway Protocol (EGP).</li> <li>?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</li> </ul>
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the <b>set local-preference</b> route-map configuration command. The default value is 100.

**Table 120** *show bgp ipv6 neighbors advertised-routes and routes Field Descriptions (continued)*

Field	Description
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

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

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
```

```
Address      Refcount Metric Path
0x6131D7DC   2         0 293 3425 2500 i
0x6132861C   2         0 293 7610 i
0x6131AD18   2         0 293 3425 4697 i
0x61324084   2         0 293 1275 3748 i
0x61320E0C   1         0 293 3425 2500 2497 i
0x61326928   1         0 293 3425 2513 i
0x61327BC0   2         0 293 i
0x61321758   1         0 293 145 i
0x61320BEC   1         0 293 3425 6509 i
0x6131AAF8   2         0 293 1849 2914 ?
0x61320FE8   1         0 293 1849 1273 209 i
0x613260A8   2         0 293 1849 i
0x6132586C   1         0 293 1849 5539 i
0x6131BBF8   2         0 293 1849 1103 i
0x6132344C   1         0 293 4554 1103 1849 1752 i
0x61324150   2         0 293 1275 559 i
0x6131E5AC   2         0 293 1849 786 i
0x613235E4   1         0 293 1849 1273 i
0x6131D028   1         0 293 4554 5539 8627 i
0x613279E4   1         0 293 1275 3748 4697 3257 i
0x61320328   1         0 293 1849 1273 790 i
0x6131EC0C   2         0 293 1275 5409 i
```

**Note**

The caret (^) symbol in the example is a regular expression that is entered by simultaneously pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

[Table 121](#) describes the significant fields shown in the display.

**Table 121** *show bgp ipv6 neighbors paths Field Descriptions*

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

The following sample output from the **show bgp ipv6 neighbors** command shows the dampened routes for IPv6 address 3FFE:700:20:1::11:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 dampened-routes
```

```
BGP table version is 32084, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
      Network          From           Reuse      Path
*d 3FFE:8030::/28    3FFE:700:20:1::11 00:24:20 293 1275 559 8933 i
```

The following sample output from the **show bgp ipv6 neighbors** command shows the flap statistics for IPv6 address 3FFE:700:20:1::11:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 flap-statistics
```

```
BGP table version is 32084, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
      Network          From           Flaps Duration Reuse      Path
*d 2001:668::/35      3FFE:700:20:1:: 4923 2d12h    00:59:50 293 1849 3257
*d 3FFE::/24          3FFE:700:20:1:: 4799 2d12h    00:59:30 293 1849 5609 4554
*d 3FFE:8030::/28    3FFE:700:20:1:: 95    11:48:24 00:23:20 293 1275 559 8933
```

The following sample output from the **show bgp ipv6 neighbors** command shows the received routes for IPv6 address 2000:0:0:4::2:

```
Router# show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
```

```
BGP table version is 2443, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network          Next Hop          Metric LocPrf Weight Path
*> 2000:0:0:1::/64 2000:0:0:4::2    0 2 1 i
*> 2000:0:0:2::/64 2000:0:0:4::2    0 2 i
*> 2000:0:0:2:1::/80 2000:0:0:4::2    0 2 ?
*> 2000:0:0:3::/64 2000:0:0:4::2    0 2 ?
* 2000:0:0:4::1/64 2000:0:0:4::2    0 2 ?
```

## Related Commands

Command	Description
<b>neighbor activate</b>	Enables the exchange of information with a neighboring router.

# show bgp ipv6 paths

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

```
show bgp ipv6 {unicast | multicast} paths regular-expression
```

Syntax Description	unicast	Specifies IPv6 unicast address prefixes.
	multicast	Specifies IPv6 multicast address prefixes.
	regular-expression	Regular expression that is used to match the received paths in the database.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.3(2)T	The <b>unicast</b> keyword was added.
	12.0(26)S	The <b>unicast</b> and <b>multicast</b> keywords were added.
	12.3(4)T	The <b>multicast</b> keyword was added.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

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

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

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

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

**Note**

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

```
Router# show bgp ipv6 unicast paths
```

```
Address      Hash Refcount Metric Path
0x61322A78   0      2      0    i
0x6131C214   3      2      0 6346 8664 786 i
0x6131D600  13      1      0 3748 1275 8319 1273 209 i
0x613229F0  17      1      0 3748 1275 8319 12853 i
0x61324AE0  18      1      1 4554 3748 4697 5408 i
0x61326818  32      1      1 4554 5609 i
0x61324728  34      1      0 6346 8664 9009 ?
0x61323804  35      1      0 3748 1275 8319 i
0x61327918  35      1      0 237 2839 8664 ?
0x61320504  38      2      0 3748 4697 1752 i
0x61320988  41      2      0 1849 786 i
0x6132245C  46      1      0 6346 8664 4927 i
```

Table 122 describes the significant fields shown in the display.

**Table 122** *show bgp ipv6 paths Field Descriptions*

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

# show bgp ipv6 peer-group

To display information about Border Gateway Protocol (BGP) peer groups, use the **show bgp ipv6 peer-group** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} peer-group [name]
```

## Syntax Description

<b>unicast</b>	Specifies IPv6 unicast address prefixes.
<b>multicast</b>	Specifies IPv6 multicast address prefixes.
<i>name</i>	(Optional) Peer group name.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The <b>unicast</b> and <b>multicast</b> keywords were added.
12.3(4)T	The <b>unicast</b> and <b>multicast</b> keywords were added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

## Usage Guidelines

If a user does not specify a peer group name, then all BGP peer groups will be displayed.

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

## Examples

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

```
Router# show bgp ipv6 unicast peer-group

BGP peer-group is external-peering, remote AS 20
  BGP version 4
  Default minimum time between advertisement runs is 30 seconds

For address family:IPv6 Unicast
  BGP neighbor is external-peering, peer-group external, members:
  1::1
  Index 0, Offset 0, Mask 0x0
  Update messages formatted 0, replicated 0
  Number of NLRI in the update sent:max 0, min 0
```

[Table 123](#) describes the significant fields shown in the display.

**Table 123** *show bgp ipv6 peer-group Field Descriptions*

<b>Field</b>	<b>Description</b>
BGP peer-group is	Type of BGP peer group.
remote AS	Autonomous system of the peer group.
BGP version	BGP version being used to communicate with the remote router.
For address family: IPv4 Unicast	IPv6 unicast-specific properties of this neighbor.

# show bgp ipv6 prefix-list

To display routes that match a prefix list, use the **show bgp ipv6 prefix-list** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} prefix-list name
```

Syntax Description	unicast	Specifies IPv6 unicast address prefixes.
	multicast	Specifies IPv6 multicast address prefixes.
	name	The specified prefix list.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	12.3(2)T	This command was introduced.
	12.0(26)S	The <b>unicast</b> and <b>multicast</b> keywords were added.
	12.3(4)T	The <b>unicast</b> and <b>multicast</b> keywords were added.

Usage Guidelines	<p>The specified prefix list must be an IPv6 prefix list, which is similar in format to an IPv4 prefix list.</p> <p>The <b>multicast</b> keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the <b>unicast</b> or <b>multicast</b> keyword is mandatory starting with Cisco IOS Release 12.0(26)S.</p>
------------------	---

**Examples** The following is sample output from the **show bgp ipv6 prefix-list** command:

```
Router# show bgp ipv6 unicast prefix-list pin

ipv6 prefix-list pin:
  count:4, range entries:3, sequences:5 - 20, refcount:2
  seq 5 permit 747::/16 (hit count:1, refcount:2)
  seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
  seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
  seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)

The ipv6 prefix-list match the following prefixes:

  seq 5: matches the exact match 747::/16
  seq 10: first 32 bits in prefix must match with a prefixlen of /64
  seq 15: first 32 bits in prefix must match with any prefixlen up to /128
  seq 20: first 16 bits in prefix must match with any prefixlen up to /124
```

[Table 124](#) describes the significant fields shown in the display.

**Table 124** *show bgp ipv6 prefix-list Field Descriptions*

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> <li>• s—The table entry is suppressed.</li> <li>• d—The table entry is dampened.</li> <li>• h—The table entry is history.</li> <li>• *—The table entry is valid.</li> <li>• &gt;—The table entry is the best entry to use for that network.</li> <li>• i—The table entry was learned via an internal BGP session.</li> </ul>
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> <li>• i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a <b>network</b> router configuration command.</li> <li>• e—Entry originated from the Exterior Gateway Protocol (EGP).</li> <li>• ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</li> </ul>
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the <b>set local-preference</b> route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

# show bgp ipv6 quote-regexp

To display IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression as a quoted string of characters, use the **show bgp ipv6 quote-regexp** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} quote-regexp regular-expression
```

## Syntax Description

<b>unicast</b>	Specifies IPv6 unicast address prefixes.
<b>multicast</b>	Specifies IPv6 multicast address prefixes.
<i>regular-expression</i>	Regular expression that is used to match the BGP autonomous system paths.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The <b>unicast</b> keyword was added.
12.0(26)S	The <b>unicast</b> and <b>multicast</b> keywords were added.
12.3(4)T	The <b>multicast</b> keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

## Usage Guidelines

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

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

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

## Examples

The following is sample output from the **show bgp ipv6 quote-regexp** command that shows paths beginning with 33 or containing 293:

**Note**

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

```
Router# show bgp ipv6 unicast quote-regexp ^33|293
```

```
BGP table version is 69964, local router ID is 192.31.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
* 2001:200::/35     3FFE:C00:E:4::2    1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                0 3320 293 3425 2500 i
* 2001:208::/35     3FFE:C00:E:4::2    1             0 4554 293 7610 i
* 2001:228::/35     3FFE:C00:E:F::2    0 6389 1849 293 2713 i
* 3FFE::/24         3FFE:C00:E:5::2    0 33 1849 4554 i
* 3FFE:100::/24     3FFE:C00:E:5::2    0 33 1849 3263 i
* 3FFE:300::/24     3FFE:C00:E:5::2    0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2    0 6389 1849 293 1275
```

**Note**

The caret (^) symbol in the example is a regular expression that is entered by pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

Table 125 describes the significant fields shown in the display.

**Table 125** *show bgp ipv6 quote-regexp Field Descriptions*

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> <li>s—The table entry is suppressed.</li> <li>d—The table entry is dampened.</li> <li>h—The table entry is history.</li> <li>*—The table entry is valid.</li> <li>&gt;—The table entry is the best entry to use for that network.</li> <li>i—The table entry was learned via an internal BGP session.</li> </ul>

**Table 125** *show bgp ipv6 quote-regexp Field Descriptions (continued)*

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> <li>• i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a <b>network</b> router configuration command.</li> <li>• e—Entry originated from the Exterior Gateway Protocol (EGP).</li> <li>• ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</li> </ul>
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the <b>set local-preference</b> route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

**Related Commands**

Command	Description
<b>show bgp ipv6 regexp</b>	Displays IPv6 BGP routes matching the autonomous system path regular expression.
<b>show ip bgp regexp</b>	Displays routes matching the regular expression.

# show bgp ipv6 regex

To display IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression, use the **show bgp ipv6 regex** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} regex regular-expression
```

Syntax Description		
<b>unicast</b>		Specifies IPv6 unicast address prefixes.
<b>multicast</b>		Specifies IPv6 multicast address prefixes.
<i>regular-expression</i>		Regular expression that is used to match the BGP autonomous system paths.

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.3(2)T	The <b>unicast</b> keyword was added.
	12.0(26)S	The <b>unicast</b> and <b>multicast</b> keywords were added.
	12.3(4)T	The <b>multicast</b> keyword was added.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines	
	The <b>show bgp ipv6 unicast regex</b> and <b>show bgp ipv6 multicast regex</b> commands provide output similar to the <b>show ip bgp regex</b> command, except they are IPv6-specific.
	The <b>unicast</b> keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the <b>unicast</b> keyword is mandatory starting with Cisco IOS Release 12.3(2)T.
	The <b>multicast</b> keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the <b>unicast</b> or <b>multicast</b> keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples	
	The following is sample output from the <b>show bgp ipv6 regex</b> command that shows paths beginning with 33 or containing 293:

**Note**

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

```
Router# show bgp ipv6 unicast regexp ^33|293
```

```
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2      1             0 4554 293 3425 2500 i
*
*                  2001:0DB8:0:F004::1
*
*  2001:208::/35    3FFE:C00:E:4::2      1             0 3320 293 3425 2500 i
*  2001:228::/35    3FFE:C00:E:F::2      0 6389 1849 293 2713 i
*  3FFE::/24         3FFE:C00:E:5::2      0 33 1849 4554 i
*  3FFE:100::/24     3FFE:C00:E:5::2      0 33 1849 3263 i
*  3FFE:300::/24     3FFE:C00:E:5::2      0 33 293 1275 1717 i
*
*                  3FFE:C00:E:F::2      0 6389 1849 293 1275
```

**Note**

The caret (^) symbol in the example is a regular expression that is entered by pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

Table 126 describes the significant fields shown in the display.

**Table 126** show bgp ipv6 regexp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> <li>s—The table entry is suppressed.</li> <li>d—The table entry is dampened.</li> <li>h—The table entry is history.</li> <li>*—The table entry is valid.</li> <li>&gt;—The table entry is the best entry to use for that network.</li> <li>i—The table entry was learned via an internal BGP session.</li> </ul>

**Table 126** *show bgp ipv6 regexp Field Descriptions (continued)*

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> <li>• i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a <b>network</b> router configuration command.</li> <li>• e—Entry originated from the Exterior Gateway Protocol (EGP).</li> <li>• ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</li> </ul>
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the <b>set local-preference</b> route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

# show bgp ipv6 route-map

To display IPv6 Border Gateway Protocol (BGP) routes that failed to install in the routing table, use the **show bgp ipv6 route-map** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} route-map name
```

Syntax Description	unicast	Specifies IPv6 unicast address prefixes.
	multicast	Specifies IPv6 multicast address prefixes.
	name	A specified route map to match.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	12.3(2)T	This command was introduced.
	12.0(26)S	The <b>unicast</b> and <b>multicast</b> keywords were added.
	12.3(4)T	The <b>unicast</b> and <b>multicast</b> keywords were added.

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

**Examples** The following is sample output from the **show bgp ipv6 route-map** command for a route map named rmap:

```
Router# show bgp ipv6 unicast route-map rmap

BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*>i12:12::/64      2001:0DB8:101::1      0     100   50 ?
*>i12:13::/64      2001:0DB8:101::1      0     100   50 ?
*>i12:14::/64      2001:0DB8:101::1      0     100   50 ?
*>i543::/64        2001:0DB8:101::1      0     100   50 ?
```

Table 127 describes the significant fields shown in the display.

**Table 127** *show bgp ipv6 route-map Field Descriptions*

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> <li>• s—The table entry is suppressed.</li> <li>• d—The table entry is dampened.</li> <li>• h—The table entry is history.</li> <li>• *—The table entry is valid.</li> <li>• &gt;—The table entry is the best entry to use for that network.</li> <li>• i—The table entry was learned via an internal BGP session.</li> <li>• r —A RIB failure has occurred.</li> <li>• S—The route map is stale.</li> </ul>
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> <li>• i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a <b>network</b> router configuration command.</li> <li>• e—Entry originated from the Exterior Gateway Protocol (EGP).</li> <li>• ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</li> </ul>
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the <b>set local-preference</b> route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

# show bgp ipv6 summary

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

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

Syntax Description	unicast	Specifies IPv6 unicast address prefixes.
	multicast	Specifies IPv6 multicast address prefixes.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.3(2)T	The <b>unicast</b> keyword was added.
	12.0(26)S	The <b>unicast</b> and <b>multicast</b> keywords were added.
	12.3(4)T	The <b>unicast</b> and <b>multicast</b> keywords were added.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines	<p>The <b>show bgp ipv6 unicast summary</b> and <b>show bgp ipv6 multicast summary</b> commands provide output similar to the <b>show ip bgp summary</b> command, except they are IPv6-specific.</p> <p>The <b>unicast</b> keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the <b>unicast</b> keyword is mandatory starting with Cisco IOS Release 12.3(2)T.</p> <p>The <b>multicast</b> keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the <b>unicast</b> or <b>multicast</b> keyword is mandatory starting with Cisco IOS Release 12.0(26)S.</p>
------------------	--

Examples	The following is sample output from the <b>show bgp ipv6 summary</b> command:
----------	---

**Note**

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

```
Router# show bgp ipv6 unicast summary
```

```
BGP router identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
```

```
Neighbor          V    AS  MsgRcvd  MsgSent   TblVer   InQ   OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2  4    200    6869    6882      0     0     0  06:25:24  Active
```

Table 128 describes the significant fields shown in the display.

**Table 128** *show bgp ipv6 summary Field Descriptions*

Field	Description
BGP router identifier	IP address of the networking device.
BGP table version	Internal version number of the BGP database.
main routing table version	Last version of BGP database that was injected into the main routing table.
Neighbor	IPv6 address of a neighbor.
V	BGP version number spoken to that neighbor.
AS	Autonomous system.
MsgRcvd	BGP messages received from that neighbor.
MsgSent	BGP messages sent to that neighbor.
TblVer	Last version of the BGP database that was sent to that neighbor.
InQ	Number of messages from that neighbor waiting to be processed.
OutQ	Number of messages waiting to be sent to that neighbor.
Up/Down	The length of time that the BGP session has been in state Established, or the current state if it is not Established.
State/PfxRcd	Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the <b>neighbor maximum-prefix</b> command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle.  An (Admin) entry with Idle status indicates that the connection has been shut down using the <b>neighbor shutdown</b> command.

**Related Commands**

Command	Description
<b>clear bgp ipv6</b>	Resets an IPv6 BGP TCP connection using BGP soft reconfiguration.
<b>neighbor maximum-prefix</b>	Controls how many prefixes can be received from a neighbor.
<b>neighbor shutdown</b>	Disables a neighbor or peer group.

# show bgp vpnv6 unicast

To display Virtual Private Network (VPN) entries in a Border Gateway Protocol (BGP) table, use the **show bgp vpnv6 unicast** command in user EXEC or privileged EXEC mode.

```
show bgp vpnv6 unicast [all | vrf [vrf-name]]
```

Syntax Description	all	(Optional) Displays all entries in a BGP table.
	vrf	(Optional) Specifies all VPN routing and forwarding (VRF) instance tables or a specific VRF table for IPv4 or IPv6 address.
	vrf-name	(Optional) Names a specific VRF table for an IPv4 or IPv6 address.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

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

**Usage Guidelines** BGP is used for distributing VPN IPv6 routing information in the VPN backbone. The local routes placed in the BGP routing table on an egress provider edge (PE) router are distributed to other PE routers.

**Examples** The following examples shows BGP entries from all of the customer-specific IPv6 routing tables:

```
Router# show bgp vpnv6 unicast all

Network                Next Hop                Metric LocPrf  Weight Path
Route Distinguisher: 100:1
* 2001:100:1:1000::/56  2001:100:1:1000::72a    0           0      200 ?
*                       ::                      0           32768 ?
* i2001:100:1:2000::/56  ::FFFF:200.10.10.1
Route Distinguisher: 200:1
* 2001:100:2:1000::/56  ::                      0           32768 ?
* 2001:100:2:2000::/56  ::FFFF:200.10.10.1    0           32768 ?
```

[Table 129](#) describes the significant fields shown in the displays.

**Table 129** *show bgp vpnv6 unicast Field Descriptions*

Field	Description
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
Loc Prf	Local preference value as configured with the <b>set local-preference</b> command.
Weight	Weight of the route as set through autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. It can be one of the following values: <ul style="list-style-type: none"> <li>• i—The entry was originated with the IGP and advertised with a network router configuration command.</li> <li>• e—The route originated with EGP.</li> <li>• ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.</li> </ul>
Route Distinguisher:	Specifies the VRF instance.

# show call active fax

To display call information for T.37 store-and-forward fax transmissions in progress, use the **show call active fax** command in user EXEC or privileged EXEC mode.

```
show call active fax [brief [id identifier] | compact [duration {less seconds | more seconds}]
                    | id identifier]
```

Syntax Description	
<b>brief</b>	(Optional) Displays a truncated version of fax call information.
<b>id identifier</b>	(Optional) Displays only the call with the specified <i>identifier</i> . Range is a hex value from 1 to FFFF.
<b>compact</b>	(Optional) Displays a compact version of the fax call information.
<b>duration</b>	(Optional) Displays active calls that are longer or shorter than a specified <i>seconds</i> value. The arguments and keywords are as follows: <ul style="list-style-type: none"> <li>• <b>less</b>—Displays calls shorter than the <i>seconds</i> value.</li> <li>• <b>more</b>—Displays calls longer than the <i>seconds</i> value.</li> <li>• <i>seconds</i>—Elapsed time, in seconds. Range is from 1 to 2147483647. There is no default value.</li> </ul>

Command Modes	
	User EXEC (>) Privileged EXEC (#)

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
	12.0(3)XG	This command was modified. Support for Voice over Frame Relay (VoFR) was added.
	12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
	12.0(4)T	This command was implemented on the Cisco 7200 series.
	12.0(7)XK	This command was implemented on the Cisco MC3810.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
	12.1(3)T	This command was modified. This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
	12.1(5)XM	This command was implemented on the Cisco AS5800.
	12.1(5)XM2	The 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 integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
	12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Release	Modification
12.3(14)T	This command was modified. T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through vendor-specific attributes (VSAs) and added to the call log.
12.4(2)T	This command was modified. The LocalHostname display field was added to the VoIP call leg record.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

### Usage Guidelines

Use this command to display the contents of the active call table. This command displays information about call times, dial peers, connections, quality of service, and other status and statistical information for T.37 store-and-forward fax calls currently connected through the router. This command works with both on-ramp and off-ramp store-and-forward fax functions.

To display information about fax relay calls in progress, use the **show call active voice** command.

### Examples

The following is sample output from the **show call active fax** command:

```
Router# show call active fax

GENERIC:
SetupTime=22021 ms
Index=1
PeerAddress=peer one
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=24284
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=10
TransmitPackets=0
TransmitBytes=0
ReceivePackets=0
ReceiveBytes=41190

MMOIP:
ConnectionId[0x37EC7F41 0xB0110001 0x0 0x35C34]
CallID=1
RemoteIPAddress=10.0.0.0
SessionProtocol=SMTP
SessionTarget=
MessageId=
AccountId=
ImgEncodingType=MH
ImgResolution=fine
AcceptedMimeTypes=2
DiscardedMimeTypes=1
Notification=None
```

```

GENERIC:
SetupTime=23193 ms
Index=1
PeerAddress=527....
PeerSubAddress=
PeerId=3469
PeerIfIndex=157
LogicalIfIndex=30
ConnectTime=24284
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=10
TransmitPackets=5
TransmitBytes=6513
ReceivePackets=0
ReceiveBytes=0

TELE:
ConnectionId=[0x37EC7F41 0xB0110001 0x0 0x35C34]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
TxDuration=24010 ms
FaxTxDuration=10910 ms
FaxRate=14400
NoiseLevel=-1
ACOMLevel=-1
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=-1
SessionTarget=
ImgPages=0

```

Table 130 provides an alphabetical listing of the fields displayed in the output of the **show call active fax** command and a description of each field.

**Table 130** *show call active fax Field Descriptions*

Field	Description
ACOM Level	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
Buffer Drain Events	Total number of jitter buffer drain events.
Buffer Fill Events	Total number of jitter buffer fill events.
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.

**Table 130** *show call active fax Field Descriptions (continued)*

Field	Description
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in milliseconds, at which the call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet-loss events.
Corrected packet-loss Events	Total number of packet-loss events that were corrected using the RFC 2198 method.
Dial-Peer	Tag of the dial peer sending this call.
EchoCancellerMaxReflector=64	The location of the largest reflector, in milliseconds (ms). The reflector size does not exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report beyond 32 ms.
ERLLevel	Current echo return loss (ERL) level for this call.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPayoutDelay	High-water-mark Voice Payout FIFO Delay during this call, in ms.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Elapsed time since the last jitter buffer drain or fill event, in seconds.
LocalHostname	Local hostnames used for locally generated gateway URLs.

**Table 130** *show call active fax Field Descriptions (continued)*

Field	Description
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPayoutDelay	Low-water-mark Voice Payout FIFO Delay during this call, in ms.
LowerIFName	Physical lower interface information. Appears only if the medium is ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR, or HDLC.
Modem passthrough signaling method in use	Indicates that this is a modem pass-through call and that named signaling events (NSEs)—a Cisco-proprietary version of named telephone events in RFC 2833—are used for signaling codec upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
NoiseLevel	Active noise level for this call.
OnTimeRvPayout	Duration of voice payout from data received on time for this call. Derive the Total Voice Payout Duration for Active Voice by adding the OnTimeRvPayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
Percent Packet Loss	Total percent packet loss.
Port	Identification of the time-division multiplexing (TDM) voice port carrying the call.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Payout FIFO Delay plus the Decoder Delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
ReleaseSource	Number value of the release source.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.

**Table 130** *show call active fax Field Descriptions (continued)*

Field	Description
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in milliseconds, when the call associated with this entry was started.
SignalingType	Signaling type for this call; for example, channel-associated signaling (CAS) or common channel signaling (CCS).
SIP call-legs	Total Session Initiation Protocol (SIP) call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call active fax brief** command:

```
Router# show call active fax brief

<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state> \
  tx:<packets>/<bytes> rx:<packets>/<bytes> <state>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  sig:<on/off> <codec> (payload size)
Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm

1      : 22021hs.1 +2263 pid:0 Answer wook song active
tx:0/0 rx:0/41190
IP 0.0.0.0 AcceptedMime:2 DiscardedMime:1

1      : 23193hs.1 +1091 pid:3469 Originate 527.... active
tx:10/13838 rx:0/0
Tele : tx:31200/10910/20290ms noise:-1 acom:-1 i/o:0/0 dBm
```

The following is sample output from the **show call active fax** command displaying T.38 fax relay statistics:

```
Router# show call active fax

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Multicast call-legs: 0
```

## show call active fax

```

Total call-legs: 1

  GENERIC:
SetupTime=1874690 ms
Index=1
PeerAddress=5551234
PeerSubAddress=
PeerIG=3
PeerIfIndex=244
LogicalIfIndex=118
ConnectTime=187875
CallDuration=00:00:44 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=fax
TransmitPackets=309
TransmitBytes=5661
ReceivePackets=1124
ReceiveBytes=49189
  TELE:
ConnectionId=[0x6B241E98 0xA78111D8 0x8002000A 0xF4107CA0]
IncomingConnectionId=[0x6B241E98 0xA78111D8 0x8002000A 0xF4107CA0]
CallID=1
Port=3/0/0 (1)
BearerChannel=3/0/0.1
TxDuration=2840 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
FaxRate=disable bps
FaxRelayMaxJitBufDepth 346
FaxRelayJitterBufOverflow 0
Initial HS Modulation is V.17/long/14400
Recent HS modulation is V.17/short/14400
Number of pages 1
Direction of transmission is Transmit
Num of Packets TX'ed/RX'ed 932/52
Packet loss conceal is 0
Encapsulation protocol is T.38 (UDPTL)
ECM is DISABLED
NoiseLevel=0
ACOMLevel=0
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=0
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=5551234
OriginalCallingOctet=0x80
OriginalCalledNumber=5555678
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=5551234
TranslatedCallingOctet=0x80
TranslatedCalledNumber=5555678
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=5555678
GwReceivedCalledOctet3=0x80

```

```
GwReceivedCallingNumber=5551234
GwReceivedCallingOctet3=0x80
GwReceivedCallingOctet3a=0x0
DSPIdentifier=1/0:0
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
```

**Table 131** provides an alphabetical listing of the fields displayed in the output of the **show call active fax** command for T.38 fax relay statistics and a description of each field.

**Table 131** *show call active fax Field Descriptions for Significant T.38 Fax Relay Statistics*

Field	Description
ACOMLevel	Current ACOM level estimate in 0.1 dB increments. The term ACOM is used in G.165, <i>General Characteristics of International Telephone Connections and International Telephone Circuits: Echo Cancellers</i> . ACOM is the combined loss achieved by the echo canceller, which is the sum of the ERL, ERL enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
ERLLevel	Current ERL level estimate in 0.1 dB increments.
FaxRate	Fax transmission rate from this peer to the specified dial peer, in bits per second (bps).
FaxRelayJitterBufOverflow	Fax relay jitter buffer overflow, in ms.
FaxRelayMaxJitBufDepth	Fax relay maximum jitter buffer depth, in ms.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call, in ms.
GwReceivedCalledNumber, GwReceivedCalledOctet3	Call information received at the gateway.
H323 call-legs	Type of call: H.323.
Initial HS Modulation	Initial high speed modulation used.
LogicalIfIndex	Index number of the logical interface for this call.
MGCP call-legs	Type of call: Media Gateway Control Protocol (MGCP).
Multicast call-legs	Type of call: Multicast.
OriginalCallingNumber, OriginalCalling Octet, OriginalCalledNumber, OriginalCalledOctet, OriginalRedirectCalledNumber, OriginalRedirectCalledOctet	Original call information regarding calling, called, and redirect numbers, and octet-3s. Octet-3s are information elements (IEs) of Q.931 that include type of number, numbering plan indicator, presentation indicator, and redirect reason information.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
Port	Identification of the TDM voice port carrying the call.
Recent HS Modulation	Most recent high-speed modulation used.

**Table 131** *show call active fax Field Descriptions for Significant T.38 Fax Relay Statistics*

<b>Field</b>	<b>Description</b>
SIP call-legs	Type of call: SIP.
Telephony call-legs	Type of call: Telephony.
Total call-legs	Total calls.
TranslatedCallingNumber, TranslatedCallingOctet, TranslatedCalledNumber, TranslatedCalledOctet, TranslatedRedirectCalledNumber, TranslatedRedirectCalledOctet	Translated call information.
TxDuration	Duration of transmit path open from this peer to the voice gateway for this call, in ms.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show call active voice</b>	Displays call information for voice calls that are in progress.
<b>show call history</b>	Displays the call history table.
<b>show call-router routes</b>	Displays the dynamic routes in the cache of the BE.
<b>show call-router status</b>	Displays the Annex G BE status.
<b>show voice port</b>	Displays configuration information about a specific voice port.

# show call active voice

To display call information for voice calls in progress, use the **show call active voice** command in user EXEC or privileged EXEC mode.

```
show call active voice [[brief] [long-dur-call-inactive | media-inactive] [called-number number
| calling-number number] [id call-identifier] | compact [duration {less | more} seconds] |
echo-canceller {hexadecimal-id | port slot-number | summary} | long-dur-call
[called-number number | calling-number number] | redirect tbct | stats]
```

## Syntax in Cisco IOS Release 12.2(33)SXH and Subsequent 12.2SX Releases

```
show call active [brief]
```

### Syntax Description

<b>brief</b>	(Optional) Displays a truncated version of call information.
<b>long-dur-call-inactive</b>	(Optional) Displays long duration calls that are detected and notified.
<b>media-inactive</b>	(Optional) Displays information about inactive media that have been detected.
<b>called-number</b> <i>number</i>	(Optional) Displays a specific called number pattern.
<b>calling-number</b> <i>number</i>	(Optional) Displays a specific calling number pattern.
<b>id</b> <i>call-identifier</i>	(Optional) Displays only the call with the specified <i>call-identifier</i> value. The range is from 1 to FFFF.
<b>compact</b>	(Optional) Displays a compact version of call information.
<b>duration</b>	(Optional) Displays the call history for the specified time duration.
<b>less</b> <i>seconds</i>	Displays the call history for shorter duration calls, in seconds. The range is from 1 to 2147483647.
<b>more</b> <i>seconds</i>	Displays the call history for longer duration calls, in seconds. The range is from 1 to 2147483647.
<b>echo-canceller</b>	(Optional) Displays information about the state of the extended echo canceller (EC).
<i>hexadecimal-id</i>	The hexadecimal ID of an active voice call. The range is from 0x0 to 0xFFFFFFFF.
<b>port</b> <i>slot-number</i>	Displays EC details for a specified active voice port. The range varies depending on the voice ports available on the router.
<b>summary</b>	Displays an EC summary for all active voice calls.
<b>long-dur-call</b>	(Optional) Displays long duration calls that are detected and notified.
<b>redirect</b>	(Optional) Displays information about active calls that are being redirected using Release-to-Pivot (RTPvt) or Two B-Channel Transfer (TBCT).
<b>tbct</b>	Displays information about TBCT calls.
<b>stats</b>	(Optional) Displays information about digital signal processing (DSP) voice quality metrics.

### Command Modes

User EXEC (>)  
Privileged EXEC (#)

Command History	Release	Modification
	11.3(1)T	This command was introduced.
	12.0(3)XG	This command was modified. Support for Voice over Frame Relay (VoFR) was added.
	12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
	12.0(4)T	This command was implemented on the Cisco 7200 series.
	12.0(7)XK	This command was implemented on the Cisco MC3810.
	12.1(3)T	This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
	12.1(5)XM	This command was implemented on the Cisco AS5800.
	12.1(5)XM2	The 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 integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
	12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
	12.2(13)T	This command was modified. The <b>echo-canceller</b> keyword was added. The command output was modified with an extra reflector location when the extended EC is present; the largest reflector location is shown.
	12.3(1)	This command was modified. The <b>redirect</b> keyword was added.
	12.3(4)T	This command was modified. The <b>called-number</b> , <b>calling-number</b> , and <b>media-inactive</b> keywords were added.
	12.3(14)T	This command was modified. New output relating to Skinny Client Control Protocol (SCCP), SCCP Telephony Control Application (STCAPP), and modem pass-through traffic was added.
	12.4(2)T	This command was modified. The LocalHostname display field was added to the VoIP call leg record and command output was enhanced to display modem relay physical layer and error correction protocols.
	12.4(4)T	This command was modified. The <b>long-dur-call</b> keyword was added.
	12.4(11)XW	This command was modified. The <b>stats</b> keyword was added.
	12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
	12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

### Usage Guidelines

Use this command to display the contents of the active voice call table. This command displays information about call times, dial peers, connections, and quality of service, and other status and statistical information for voice calls currently connected through the router.

Before you can query the echo state, you need to know the hexadecimal ID. To find the hexadecimal ID, enter the **show call active voice brief** command or use the **show voice call status** command.

When the extended EC is present, the **show call active voice** command displays the contents of the Ditech EC\_CHAN\_CTRL structure. Table 132 contains names and descriptions of the fields in the EC\_CHAN\_CTRL structure. Table 132 also provides a listing of the information types associated with this command.

**Table 132** EC\_CHAN\_CTRL Field Descriptions

Symbol	Field	Description
BYPO	Channel bypass	<ul style="list-style-type: none"> <li>1 = Transparent bypass; EC is disabled.</li> <li>0 = Cancel; EC is enabled.</li> </ul>
TAIL3	Max tail	<ul style="list-style-type: none"> <li>0 = 24 milliseconds.</li> <li>1 = 32 milliseconds.</li> <li>2 = 48 milliseconds.</li> <li>3 = 64 milliseconds.</li> </ul> <p><b>Note</b> This field should be set just greater than the anticipated worst round-trip tail delay.</p>
REC3	Residual echo control	<ul style="list-style-type: none"> <li>0 = Cancel only; echo is the result of linear processing; no nonlinear processing is applied.</li> <li>1 = Suppress residual; residual echo is zeroed; simple nonlinear processing is applied (you might experience “dead air” when talking).</li> <li>2 = Reserved.</li> <li>3 = Generate comfort noise (default).</li> </ul>
FRZ0	h-register hold	1 = Freezes h-register; used for testing.
HZ0	h-register clear	Sending the channel command with this bit set clears the h-register.
TD3	Modem tone disable	<ul style="list-style-type: none"> <li>0 = Ignore 2100 Hz modem answer tone.</li> <li>1 = G.164 mode (bypass canceller if 2100 Hz tone).</li> <li>2 = R.</li> <li>3 = G.165 mode (bypass canceller for phase reversing tone only).</li> </ul>
ERL0	Echo return loss	<ul style="list-style-type: none"> <li>0 = 6 decibel (dB).</li> <li>1 = 3 dB.</li> <li>2 = 0 dB.</li> <li>3 = R. Worst echo return loss (ERL) situation in which canceller still works.</li> </ul>
HLC1	High level compensation	<ul style="list-style-type: none"> <li>0 = No attenuation.</li> <li>1 = 6 dB if clipped. On loud circuits, the received direction can be attenuated 6 dB if clipping is observed.</li> </ul>
R0	Reserved	Must be set to 0 to ensure compatibility with future releases.

Use the **show call active voice redirect tbct** command to monitor any active calls that implement RTPvt or TBCT.

When a call is no longer active, its record is stored. You can display the record by using the **show call history voice** command.

### Examples

The following is sample output from the **show call active voice** command for modem relay traffic:

```
Router# show call active voice

Modem Relay Local Rx Speed=0 bps
Modem Relay Local Tx Speed=0 bps
Modem Relay Remote Rx Speed=0 bps
Modem Relay Remote Tx Speed=0 bps
Modem Relay Phy Layer Protocol=v34
Modem Relay Ec Layer Protocol=v14
SPRTInfoFramesReceived=0
SPRTInfoTFramesSent=0
SPRTInfoTFramesResent=0
SPRTXidFramesReceived=0
SPRTXidFramesSent=0
SPRTTotalInfoBytesReceived=0
SPRTTotalInfoBytesSent=0
SPRTPacketDrops=0
```

Table 133 describes the significant fields shown in the display.

**Table 133** show show call active voice Field Descriptions

Field	Description
Modem Relay Local Rx Speed	Download speed, in bits per second, of the local modem relay.
Modem Relay Local Tx Speed	Upload speed of the local modem relay.
Modem Relay Remote Rx Speed	Download speed of the remote modem relay.
Modem Relay Remote Tx Speed	Upload speed of the remote modem relay.
Modem Relay Phy Layer Protocol	Physical protocol of the modem relay.
Modem Relay Ec Layer Protocol	EC layer protocol of the modem relay.
SPRTInfoFramesReceived	Total number of simple packet relay transport (SPRT) protocol frames received.
SPRTInfoTFramesSent	Total number of SPRT frames sent.
SPRTInfoTFramesResent	Total number of SPRT frames sent again.
SPRTXidFramesReceived	Total number of SPRTS ID frames received.
SPRTXidFramesSent	Total number of SPRTS ID frames sent.
SPRTTotalInfoBytesReceived	Total number of SPRT bytes received.
SPRTTotalInfoBytesSent	Total number of SPRT bytes sent.
SPRTPacketDrops	Total number of SPRT packets dropped.

The following is sample output from the **show call active voice** command:

```
Router# show call active voice

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
```

```
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

    GENERIC:
SetupTime=1072620 ms
Index=1
PeerAddress=9193927582
PeerSubAddress=
PeerId=8
PeerIfIndex=19
LogicalIfIndex=0
ConnectTime=1078940 ms
CallDuration=00:00:51 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=1490
TransmitBytes=0
ReceivePackets=2839
ReceiveBytes=56780
VOIP:
ConnectionId[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
IncomingConnectionId[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
CallID=1
RemoteIPAddress=10.44.44.44
RemoteUDPPort=17096
RemoteSignallingIPAddress=10.44.44.44
RemoteSignallingPort=56434
RemoteMediaIPAddress=10.44.44.44
RemoteMediaPort=17096
RoundTripDelay=6 ms
SelectedQoS=best-effort
tx_DtmfRelay=h245-signal
FastConnect=TRUE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=TRUE

SessionProtocol=cisco
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=54160
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=60 ms
TxPakNumber=1490
TxSignalPak=0
TxComfortNoisePak=1
TxDuration=54240
TxVoiceDuration=29790
RxPakNumber=2711
RxSignalPak=0
RxDuration=0
TxVoiceDuration=54210
VoiceRxDuration=54160
```

## show call active voice

```

RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=60
PlayDelayMin=60
PlayDelayMax=70
PlayDelayClockOffset=212491899
PlayDelayJitter=0 ms
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverflow=10
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-57
InSignalLevel=-51
LevelTxPowerMean=0
LevelRxPowerMean=-510
LevelBgNoise=0
ERLLevel=16
ACOMLevel=16
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
ReceiveDelay=60 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=9193927582
OriginalCallingOctet=0x21
OriginalCalledNumber=93615494
OriginalCalledOctet=0xC1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=9193927582
TranslatedCallingOctet=0x21
TranslatedCalledNumber=93615494
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=93615494
GwReceivedCalledOctet3=0xC1
GwReceivedCallingNumber=9193927582
GwReceivedCallingOctet3=0x21
GwReceivedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=

    GENERIC:
SetupTime=1072760 ms
Index=1
PeerAddress=93615494
PeerSubAddress=
PeerId=9

```

```
PeerIfIndex=18
LogicalIfIndex=4
ConnectTime=1078940 ms
CallDuration=00:00:53 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=2953
TransmitBytes=82684
ReceivePackets=1490
ReceiveBytes=29781
TELE:
ConnectionId=[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
IncomingConnectionId=[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
CallID=2
Port=3/0/0 (1)
BearerChannel=3/0/0.2
TxDuration=59080 ms
VoiceTxDuration=29790 ms
FaxTxDuration=0 ms
CoderTypeRate=g729r8
NoiseLevel=-54
ACOMLevel=16
OutSignalLevel=-57
InSignalLevel=-51
InfoActivity=1
ERLLevel=16
EchoCancellerMaxReflector=8
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
AlertTimepoint=1073340 ms
OriginalCallingNumber=9193927582
OriginalCallingOctet=0x21
OriginalCalledNumber=93615494
OriginalCalledOctet=0xC1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=9193927582
TranslatedCallingOctet=0x21
TranslatedCalledNumber=93615494
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=93615494
GwReceivedCalledOctet3=0xC1
GwOutpulsedCalledNumber=93615494
GwOutpulsedCalledOctet3=0xC1
GwReceivedCallingNumber=9193927582
GwReceivedCallingOctet3=0x21
GwReceivedCallingOctet3a=0x81
GwOutpulsedCallingNumber=9193927582
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
DSPIdentifier=3/1:1
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

Table 132 on page 1727 and Table 134 describe the significant fields shown in the display, in alphabetical order.

**Table 134** *show call active voice Field Descriptions*

Field	Description
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallState	Current state of the call.
Call agent controlled call-legs	Displays call legs for devices that are not telephony endpoints; for example, transcoding and conferencing
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in ms, during which the call was connected.
EchoCancellerMaxReflector	Size of the largest reflector, in ms. The reflector size cannot exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report capacity beyond 32 ms.
ERLLevel	Current echo return loss (ERL) level for this call.
FaxTxDuration	Duration, in ms, of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration, in ms, of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration, in ms, of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration, in ms, of the voice signal played out with a signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration, in ms, of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters; that is, parameters that are common for VoIP and telephony call legs.
H320CallType	Total H320 call types available.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPayoutDelay	High-water-mark voice payout first in first out (FIFO) delay during this call, in ms.

**Table 134** *show call active voice Field Descriptions*

Field	Description
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice, speech, or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayOutDelay	Low-water-mark voice playout FIFO delay during this call, in ms.
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Multicast call-legs	Total multicast call legs for which call records are available.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayOut	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayOut value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay, in ms, between the local and remote systems on the IP backbone for this call.
SCCP call-legs	Call legs for SCCP telephony endpoints.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in ms, when the call associated with this entry was started.
SIP call-legs	Total SIP call legs for which call records are available.

**Table 134** show call active voice Field Descriptions

Field	Description
Telephony call-legs	Total telephony call legs for which call records are available.
Total call-legs	Total number of call legs for the call.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call active voice** command for voice traffic over call-agent controlled call legs. Note that call legs for SCCP telephony endpoints, that is, phones controlled by STCAPP, are displayed under the “Call agent controlled call-legs” field (“SCCP call-legs” displays call legs for devices that are not telephony endpoints; for example, transcoding and conferencing).

```
Router# show call active voice
```

```
Telephony call-legs: 2
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 2
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 4

  GENERIC:
SetupTime=1557650 ms
Index=1
PeerAddress=
PeerSubAddress=
PeerId=999100
PeerIfIndex=14
LogicalIfIndex=10
ConnectTime=1562040 ms
CallDuration=00:01:01 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=3101
TransmitBytes=519564
ReceivePackets=3094
ReceiveBytes=494572
  TELE:
ConnectionId=[0x11B1860C 0x22D711D7 0x8014E4D4 0x8FD15327]
IncomingConnectionId=[0x11B1860C 0x22D711D7 0x8014E4D4 0x8FD15327]
CallID=25
Port=3/0/0 (25)
BearerChannel=3/0/0.1
TxDuration=59670 ms
VoiceTxDuration=59670 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
```

```
NoiseLevel=-12
ACOMLevel=22
OutSignalLevel=-12
InSignalLevel=-11
InfoActivity=1
ERLLevel=22
EchoCancellerMaxReflector=2
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
DSPIdentifier=1/1:1

    GENERIC:
SetupTime=1559430 ms
Index=1
PeerAddress=7702
PeerSubAddress=
PeerId=999100
PeerIfIndex=14
LogicalIfIndex=11
ConnectTime=1562020 ms
CallDuration=00:01:03 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3151
TransmitBytes=528900
ReceivePackets=3158
ReceiveBytes=503876
    TELE:
ConnectionId=[0x0 0x0 0x0 0x0]
IncomingConnectionId=[0x0 0x0 0x0 0x0]
CallID=26
Port=3/0/0 (26)
BearerChannel=3/0/0.2
TxDuration=60815 ms
VoiceTxDuration=60815 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-12
ACOMLevel=28
OutSignalLevel=-12
InSignalLevel=-11
InfoActivity=1
ERLLevel=28
EchoCancellerMaxReflector=2
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
```

## show call active voice

```

AlertTimepoint=1559430 ms
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=7701
TranslatedCallingOctet=0x0
TranslatedCalledNumber=7702
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
GwOutpulsedCalledNumber=7702
GwOutpulsedCalledOctet3=0x0
GwOutpulsedCallingNumber=7701
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x0
DSPIdentifier=1/1:2

    GENERIC:
SetupTime=1562040 ms
Index=1
PeerAddress=
PeerSubAddress=
PeerIG=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=0 ms
CallDuration=00:00:00 sec
CallState=2
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3215
TransmitBytes=512996
ReceivePackets=3208
ReceiveBytes=512812
VOIP:
ConnectionId[0x0 0x0 0x0 0x0]
IncomingConnectionId[0x0 0x0 0x0 0x0]
CallID=27
RemoteIPAddress=10.10.0.0
RemoteUDPPort=17718
RemoteSignallingIPAddress=10.10.0.0
RemoteSignallingPort=0
RemoteMediaIPAddress=10.2.6.10
RemoteMediaPort=17718
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=other
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=60640
GapFillWithSilence=0 ms

```

```
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=105 ms
LoWaterPlayoutDelay=105 ms
TxPakNumber=3040
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=60815
TxVoiceDuration=60815
RxPakNumber=3035
RxSignalPak=0
RxDuration=0
TxVoiceDuration=60690
VoiceRxDuration=60640
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=105
PlayDelayMin=105
PlayDelayMax=105
PlayDelayClockOffset=-1662143961
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverflow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-12
InSignalLevel=-11
LevelTxPowerMean=0
LevelRxPowerMean=-115
LevelBgNoise=0
ERLLevel=28
ACOMLevel=28
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
PlayoutMode = undefined
PlayoutInitialDelay=0 ms
ReceiveDelay=105 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-around

Modem passthrough signaling method is nse:
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 0sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
```

```

OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=

    GENERIC:
SetupTime=1562040 ms
Index=2
PeerAddress=
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=0 ms
CallDuration=00:00:00 sec
CallState=2
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3380
TransmitBytes=540332
ReceivePackets=3386
ReceiveBytes=540356
VOIP:
ConnectionId[0x0 0x0 0x0 0x0]
IncomingConnectionId[0x0 0x0 0x0 0x0]
CallID=28
RemoteIPAddress=10.0.0.0
RemoteUDPPort=18630
RemoteSignallingIPAddress=10.10.0.0
RemoteSignallingPort=0
RemoteMediaIPAddress=10.2.6.10
RemoteMediaPort=18630
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=FALSE

SessionProtocol=other
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=63120
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=105 ms

```

```
LoWaterPlayoutDelay=105 ms
TxPakNumber=3158
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=63165
TxVoiceDuration=63165
RxPakNumber=3164
RxSignalPak=0
RxDuration=0
TxVoiceDuration=63165
VoiceRxDuration=63120
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=105
PlayDelayMin=105
PlayDelayMax=105
PlayDelayClockOffset=957554296
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverflow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-12
InSignalLevel=-11
LevelTxPowerMean=0
LevelRxPowerMean=-114
LevelBgNoise=0
ERLLevel=22
ACOMLevel=22
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
PlayoutMode = undefined
PlayoutInitialDelay=0 ms
ReceiveDelay=105 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-around

Modem passthrough signaling method is nse:
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 0sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
```

```

OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=
Telephony call-legs: 2
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 2
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 4

```

[Table 132 on page 1727](#) and [Table 134 on page 1732](#) describe the significant fields shown in the display, in alphabetical order.

The following is sample output from the **show call active voice** command to indicate if Service Advertisement Framework (SAF) is being used:

```

Router# show call active voice

Total call-legs: 2
GENERIC:
SetupTime=1971780 ms
Index=1
PeerAddress=6046692010
PeerSubAddress=
PeerID=20003
PeerIfIndex=17
.
.
.
VOIP:
SessionProtocol=sipv2
ProtocolCallId=7A9E7D9A-EAD311DC-8036BCC4-6EEE85D6@1.5.6.12
SessionTarget=1.5.6.10
SafEnabled=TRUE
SafTrunkRouteId=1
SafPluginDialpeerTag=8

```

[Table 132 on page 1727](#) and [Table 136 on page 1744](#) describe the significant fields shown in the display.

The following is sample output from the **show call active voice** command for fax-relay traffic:

```

Router# show call active voice

Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1

GENERIC:
SetupTime=1049400 ms
Index=2
PeerAddress=52930
PeerSubAddress=

```

```
PeerId=82
PeerIfIndex=222
LogicalIfIndex=0
ConnectTime=105105
CallDuration=00:00:59
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=10
TransmitPackets=1837
TransmitBytes=29764
ReceivePackets=261
ReceiveBytes=4079
VOIP:
ConnectionId[0xEB630F4B 0x9F5E11D7 0x8008CF18 0xB9C3632]
IncomingConnectionId[0xEB630F4B 0x9F5E11D7 0x8008CF18 0xB9C3632]
RemoteIPAddress=10.7.95.3
RemoteUDPPort=16610
RemoteSignallingIPAddress=10.7.95.3
RemoteSignallingPort=1720
RemoteMediaIPAddress=10.7.95.3
RemoteMediaPort=16610
RoundTripDelay=13 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE

AnnexE=FALSE

Separate H245 Connection=FALSE

H245 Tunneling=TRUE

SessionProtocol=cisco
ProtocolCallId=
SessionTarget=ipv4:10.7.95.3
OnTimeRvPayout=1000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPayoutDelay=110 ms
LoWaterPayoutDelay=70 ms
ReceiveDelay=70 ms
LostPackets=0
EarlyPackets=1
LatePackets=0
VAD = enabled
CoderTypeRate=t38
CodecBytes=40
Media Setting=flow-through
AlertTimepoint=104972
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550130
OriginalCallingOctet=0x0
OriginalCalledNumber=52930
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x7F
TranslatedCallingNumber=4085550130
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52930
TranslatedCalledOctet=0xE9
```

```

TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52930
GwReceivedCalledOctet3=0xE9
GwOutpulsedCalledNumber=52930
GwOutpulsedCalledOctet3=0xE9
GwReceivedCallingNumber=555-0100
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
GwOutpulsedCallingNumber=555-0101
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x80
Username=
FaxRelayMaxJitterBufDepth = 0 ms
FaxRelayJitterBufOverflow = 0
FaxRelayHSmodulation = 0
FaxRelayNumberOfPages = 0
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1

```

Table 132 on page 1727 and Table 136 on page 1744 describe the significant fields shown in the display.

The following is sample output from the **show call active voice brief** command:

```
Router# show call active voice brief
```

```

<ID>: <CallID> <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>
long_duration_call_detected:<y/n> long duration call duration:n/a timestamp:n/a
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l>
i/o:<l>/<l> dBm
MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
speeds(bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>

Total call-legs:2
1269 :7587246hs.1 +260 pid:0 Answer active
  dur 00:07:14 tx:590/11550 rx:21721/434420
  IP 172.29.248.111:17394 rtt:3ms pl:431850/0ms lost:0/0/0 dela
  y:69/69/70ms g729r8

1269 :7587246hs.2 +259 pid:133001 Originate 133001 active
  dur 00:07:14 tx:21717/434340 rx:590/11550
  Tele 1/0:1 (2):tx:434350/11640/0ms g729r8 noise:-44 acom:-19
  i/o:-45/-45 dBm

```

The following is an example of the **show call active voice** command using the **echo-canceller** keyword. The number 9 represents the hexadecimal ID of an active voice call.

```
Router# show call active voice echo-canceller 9
```

```
ACOM=-65 ERL=45
Echo canceller control words=6C 0
Bypass=OFF Tail=64 Residual ecan=Comfort noise
Freeze=OFF Modem tone disable=Ignore 2100Hz tone
Worst ERL=6 High level compensation=OFF
Max amplitude reflector (in msec)=5
Ecan version = 8180
```

The following is sample output from the **show call active voice echo-canceller** command for a call with a hexadecimal ID of 10:

```
Router# show call active voice echo-canceller 10
```

```
ACOM=-15 ERL=7
Echo canceller control words=6C 0
Bypass=OFF Tail=64 Residual ecan=Comfort noise
Freeze=OFF Modem tone disable=Ignore 2100Hz tone
Worst ERL=6 High level compensation=OFF
Max amplitude reflector (in msec)=64
```

The call ID number (which is 10 in the preceding example) changes with every new active call. When an active call is up, you must enter the **show call active voice brief** command to obtain the call ID number. The call ID must be converted to hexadecimal value if you want to use the **show call active voice echo-canceller x** command ( $x$  = call ID converted to hexadecimal value).

[Table 135](#) shows call ID examples converted to hexadecimal values (generally incremented by 2):

**Table 135** Call IDs Converted to Hex

Decimal	Hex
2	2
4	4
6	6
8	8
10	A
12	C

Alternatively, you can use the **show voice call status** command to obtain the call ID. The call ID output is already in hexadecimal values form when you use this command:

```
Router# show voice call status
```

```
CallID      CID  ccVdb      Port      DSP/Ch  Called #  Codec      Dial-peers
0x1         11CE 0x02407B20 1:0.1     1/1     1000     g711ulaw   2000/1000
```

The following is sample output from the **show call active voice** command using the **compact** keyword:

```
Router# show call active voice compact
```

```
<callID>  A/O FAX T<sec> Codec      type      Peer Address      IP R<ip>:<udp>
Total call-legs: 2
58 ANS    T11          g711ulaw  VOIP      Psipp 2001:.....:230A:6080
59 ORG    T11          g711ulaw  VOIP      P5000110011      10.13.37.150:6090
```

The following is sample output from the **show call active voice redirect** command using the **tbct** keyword:

```
Router# show call active voice redirect tbct
```

```
TBCT:
```

```
Maximum no. of TBCT calls allowed:No limit
Maximum TBCT call duration:No limit
```

```
Total number TBCT calls currently being monitored = 1
```

```
ctrl name=T1-2/0, tag=13, call-ids=(7, 8), start_time=*00:12:25.985 UTC Mon Mar 1 1993
```

Table 136 describes the significant fields shown in the display.

**Table 136** *show call active voice redirect Field Descriptions*

Field	Description
Maximum no. of TBCT calls allowed	Maximum number of calls that can use TBCT as defined by the <b>tbct max calls</b> command.
Maximum TBCT call duration	Maximum length allowed for a TBCT call as defined by the <b>tbct max call-duration</b> command.
Total number TBCT calls currently being monitored	Total number of active TBCT calls.
ctrl name	Name of the T1 controller where the call originated.
tag	Call tag number that identifies the call.
call-ids	Numbers that uniquely identify the call legs.
start_time	Time, in hours, minutes, and seconds, when the redirected call began.

#### Related Commands

Command	Description
<b>show call active fax</b>	Displays call information for fax transmissions that are in progress.
<b>show call history</b>	Displays the call history table.
<b>show call-router routes</b>	Displays the dynamic routes in the cache of the BE.
<b>show call-router status</b>	Displays the Annex G BE status.
<b>show dial-peer voice</b>	Displays configuration information for dial peers.
<b>show num-exp</b>	Displays how the number expansions are configured in VoIP.
<b>show voice call status</b>	Displays the call status for voice ports on the Cisco router or concentrator.
<b>show voice port</b>	Displays configuration information about a specific voice port.

# show call history fax

To display the call history table for fax transmissions, use the **show call history fax** command in user EXEC or privileged EXEC mode.

```
show call history fax [brief [id identifier] | compact [duration {less | more} time]
                    | id identifier | last number]
```

Syntax Description	
<b>brief</b>	(Optional) Displays a truncated version of the call history table.
<b>id identifier</b>	(Optional) Displays only the call with the specified identifier. Range is a hex value from 1 to FFFF.
<b>compact</b>	(Optional) Displays a compact version.
<b>duration time</b>	(Optional) Displays history information for calls that are longer or shorter than a specified <i>time</i> value. The arguments and keywords are as follows: <ul style="list-style-type: none"> <li><b>less</b>—Displays calls shorter than the value in the <i>time</i> argument.</li> <li><b>more</b>—Displays calls longer than the value in the <i>time</i> argument.</li> <li><b>time</b>—Elapsed time, in seconds. Range is from 1 to 2147483647.</li> </ul>
<b>last number</b>	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the <i>number</i> argument. Range is from 1 to 100.

Command Modes	
	User EXEC (>)
	Privileged EXEC (#)

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series.
	12.0(3)XG	This command was implemented for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
	12.0(4)XJ	This command was modified for store-and-forward fax.
	12.0(4)T	This command was modified. The <b>brief</b> keyword was added, and the command was implemented on the Cisco 7200 series.
	12.0(7)XK	This command was modified. The <b>brief</b> keyword was implemented on the Cisco MC3810.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
	12.1(5)XM	This command was implemented on the Cisco AS5800.
	12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
	12.2(2)XA	This command was modified. The output of this command was modified to indicate whether the call in question has been established using Annex E.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	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 AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 was not included in this release.

Release	Modification
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.3(1)	This command was modified. The following fields were added: FaxRelayMaxJitterBufDepth, FaxRelayJitterBufOverflow, FaxRelayHSmodulation, and FaxRelayNumberOfPages.
12.3(14)T	This command was modified. T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through vendor-specific attributes (VSAs) and added to the call log.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

### Usage Guidelines

This command displays a call-history table that contains a list of fax calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number from 0 to 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed, also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the keyword **last**, and define the number of calls to be displayed with the *number* argument.

To display a truncated version of the call history table, use the **brief** keyword.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

### Examples

The following is sample output from the **show call history fax** command:

```
Router# show call history fax

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Total call-legs: 1

GENERIC:
SetupTime=590180 ms
Index=2
PeerAddress=4085452930
PeerSubAddress=
PeerId=81
PeerIfIndex=221
LogicalIfIndex=145
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=59389
DisconnectTime=68204
```

```

CallDuration=00:01:28
CallOrigin=2
ReleaseSource=1
ChargedUnits=0
InfoType=fax
TransmitPackets=295
TransmitBytes=5292
ReceivePackets=2967
ReceiveBytes=82110
TELE:
ConnectionId=[0xD9ACDF1 0x9F5D11D7 0x8002CF18 0xB9C3632]
IncomingConnectionId=[0xD9ACDF1 0x9F5D11D7 0x8002CF18 0xB9C3632]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
TxDuration=28960 ms
VoiceTxDuration=0 ms
FaxTxDuration=28960 ms
FaxRate=voice bps
FaxRelayMaxJitterBufDepth = 0 ms
FaxRelayJitterBufOverflow = 0
FaxRelayHSmodulation = 0
FaxRelayNumberOfPages = 0
NoiseLevel=-120
ACOMLevel=127
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550130
OriginalCallingOctet=0x0
OriginalCalledNumber=52930
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=4085550130
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52930
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52930
GwReceivedCalledOctet3=0xE9
GwReceivedCallingNumber=4085550130
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80

```

**Table 137** provides an alphabetical listing of the fields displayed in the output of the **show call history fax** command and a description of each field.

**Table 137** *show call history fax Field Descriptions*

Field	Description
ACOM Level	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
Buffer Drain Events	Total number of jitter buffer drain events.

**Table 137** *show call history fax Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Buffer Fill Events	Total number of jitter buffer fill events.
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallerName	Voice port station name string.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in milliseconds (ms), at which the call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet-loss events.
Corrected packet-loss Events	Total number of packet-loss events that were corrected using the RFC 2198 method.
Dial-Peer	Tag of the dial peer sending this call.
DisconnectCause	Cause code for the reason this call was disconnected.
DisconnectText	Descriptive text explaining the reason for the disconnect.
DisconnectTime	Time, in ms, when this call was disconnected.
EchoCancellerMaxReflector=64	The location of the largest reflector, in ms. The reflector size does not exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report beyond 32 ms.
ERLLevel	Current Echo Return Loss (ERL) level for this call.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
FaxRelayJitterBufOverFlow	Count of number of network jitter buffer overflows (number of packets). These packets are equivalent to lost packets.
FaxRelayMaxJitterBufDepth	Maximum depth of jitter buffer (in ms).
FaxRelayHSmodulation	Most recent high-speed modulation used.
FaxRelayNumberOfPages	Number of pages transmitted.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.

**Table 137** *show call history fax Field Descriptions (continued)*

Field	Description
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
GwReceivedCalledNumber, GwReceivedCalledOctet3, GwReceivedCallingNumber, GwReceivedCallingOctet3, GwReceivedCallingOctet3a	Call information received at the gateway.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark Voice Playout FIFO Delay during this call.
ImgPages	The fax pages that have been processed.
Incoming ConnectionId	The incoming_GUID. It can be different with ConnectionId (GUID) when there is a long_pound or blast_call feature involved. In those cases, incoming_GUID is unique for all the subcalls that have been generated, and GUID is different for each subcall.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Elapsed time since the last jitter buffer drain or fill event, in seconds.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark Voice Playout FIFO Delay during this call.
LowerIFName	Physical lower interface information. Appears only if the medium is ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR, or HDLC.

**Table 137** *show call history fax Field Descriptions (continued)*

Field	Description
Modem passthrough signaling method in use	Indicates that this is a modem pass-through call and that named signaling events (NSEs)—a Cisco-proprietary version of named telephone events in RFC 2833—are used for signaling codec upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
NoiseLevel	Active noise level for this call.
OnTimeRvPayout	Duration of voice payout from data received on time for this call. Derive the Total Voice Payout Duration for Active Voice by adding the OnTimeRvPayout value to the GapFill values.
OriginalCallingNumber, OriginalCalling Octet, OriginalCalledNumber, OriginalCalledOctet, OriginalRedirectCalledNumber, OriginalRedirectCalledOctet	Original call information regarding calling, called, and redirect numbers, as well as octet-3s. Octet-3s are information elements (IEs) of Q.931 that include type of number, numbering plan indicator, presentation indicator, and redirect reason information.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
Percent Packet Loss	Total percent packet loss.
Port	Identification of the voice port carrying the call.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Payout FIFO Delay plus the Decoder Delay during this voice call.
ReceivePackets	Number of packets received by this peer during this call.
ReleaseSource	Number value of the release source.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.

**Table 137** show call history fax Field Descriptions (continued)

Field	Description
SetupTime	Value of the system UpTime, in ms, when the call associated with this entry was started.
SignalingType	Signaling type for this call; for example, channel-associated signaling (CAS) or common-channel signaling (CCS).
SIP call-legs	Total SIP call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TranslatedCallingNumber, TranslatedCallingOctet, TranslatedCalledNumber, TranslatedCalledOctet, TranslatedRedirectCalled Number, TranslatedRedirectCalledOctet	Translated call information.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call history fax brief** command:

```
Router# show call history fax brief
```

```
<ID>: <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
Telephony <int>: tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm

2 : 5996450hs.25 +-1 +3802 pid:100 Answer 408
tx:0/0 rx:0/0 1F (T30 T1 EOM timeout)
Telephony : tx:38020/38020/0ms g729r8 noise:0dBm acom:0dBm

2 : 5996752hs.26 +-1 +3500 pid:110 Originate uut1@linux2.allegro.com
tx:0/0 rx:0/0 3F (The e-mail was not sent correctly. Remote SMTP server said: 354 )
IP 14.0.0.1 AcceptedMime:0 DiscardedMime:0

3 : 6447851hs.27 +1111 +3616 pid:310 Originate 576341.
tx:11/14419 rx:0/0 10 (Normal connection)
Telephony : tx:36160/11110/25050ms g729r8 noise:115dBm acom:-14dBm

3 : 6447780hs.28 +1182 +4516 pid:0 Answer
tx:0/0 rx:0/0 10 (normal call clearing.)
IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

4 : 6464816hs.29 +1050 +3555 pid:310 Originate 576341.
```

## show call history fax

```

tx:11/14413 rx:0/0 10 (Normal connection)
Telephony : tx:35550/10500/25050ms g729r8 noise:115dBm acom:-14dBm

4 : 6464748hs.30 +1118 +4517 pid:0 Answer
tx:0/0 rx:0/0 10 (normal call clearing.)
IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

5 : 6507900hs.31 +1158 +2392 pid:100 Answer 4085763413
tx:0/0 rx:3/3224 10 (Normal connection)
Telephony : tx:23920/11580/12340ms g729r8 noise:0dBm acom:0dBm

5 : 6508152hs.32 +1727 +2140 pid:110 Originate uut1@linux2.allegro.com
tx:0/2754 rx:0/0 3F (service or option not available, unspecified)
IP 14.0.0.4 AcceptedMime:0 DiscardedMime:0

6 : 6517176hs.33 +1079 +3571 pid:310 Originate 576341.
tx:11/14447 rx:0/0 10 (Normal connection)
Telephony : tx:35710/10790/24920ms g729r8 noise:115dBm acom:-14dBm

6 : 6517106hs.34 +1149 +4517 pid:0 Answer
tx:0/0 rx:0/0 10 (normal call clearing.)
IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

7 : 6567382hs.35 +1054 +3550 pid:310 Originate 576341.
tx:11/14411 rx:0/0 10 (Normal connection)
Telephony : tx:35500/10540/24960ms g729r8 noise:115dBm acom:-14dBm

7 : 6567308hs.36 +1128 +4517 pid:0 Answer
tx:0/0 rx:0/0 10 (normal call clearing.)
IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

```

The following example shows output for the **show call history fax** command with the T.38 Fax Relay statistics:

```
Router# show call history fax
```

```

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Total call-legs: 1

GENERIC:
SetupTime=9872460 ms
Index=8
PeerAddress=41023
PeerSubAddress=
PeerId=1
PeerIfIndex=242
LogicalIfIndex=180
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=9875610 ms
DisconnectTime=9936000 ms
CallDuration=00:01:00 sec
CallOrigin=2
ReleaseSource=1
ChargedUnits=0
InfoType=fax
TransmitPackets=268
TransmitBytes=4477
ReceivePackets=1650
ReceiveBytes=66882

```

```

TELE:
ConnectionId=[0xD6635DD5 0x9FA411D8 0x8005000A 0xF4107CA0]
IncomingConnectionId=[0xD6635DD5 0x9FA411D8 0x8005000A 0xF4107CA0]
CallID=7
Port=3/0/0:0 (7)
BearerChannel=3/0/0.8
TxDuration=6170 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
FaxRate=disable bps
FaxRelayMaxJitterBufDepth=560 ms
FaxRelayJitterBufOverflow=0
FaxRelayMostRecentHSmodulation=V.17/short/14400
FaxRelayNumberOfPages=1
FaxRelayInitHSmodulation=V.17/long/14400
FaxRelayDirection=Transmit
FaxRelayPktLossConceal=0
FaxRelayEcmStatus=ENABLED
FaxRelayEncapProtocol=T.38 (UDPTL)
FaxRelayNsfCountryCode=Japan
FaxRelayNsfManufCode=0031B8EE80C48511DD0D0000DDDD0000000000000000022ED00B0A400
FaxRelayFaxSuccess=Success
NoiseLevel=0
ACOMLevel=0
SessionTarget=
ImgPages=0
CallerName=Analog 41023
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x80
OriginalCalledNumber=41021
OriginalCalledOctet=0xA1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=41023
TranslatedCallingOctet=0x80
TranslatedCalledNumber=41021
TranslatedCalledOctet=0xA1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=41021
GwReceivedCalledOctet3=0xA1

```

Table 138 describes the fields not shown in Table 137.

**Table 138** show call history fax Field Descriptions

Field	Description
FaxRelayDirection	Direction of fax relay.
FaxRelayEcmStatus	Fax relay error correction mode status.
FaxRelayEncapProtocol	Fax relay encapsulation protocol.
FaxRelayFaxSuccess	Fax relay success.
FaxRelayInitHSmodulation	Fax relay initial high speed modulation.
FaxRelayMostRecentHSmodulation	Fax relay most recent high speed modulation.
FaxRelayNsfCountryCode	Fax relay Nonstandard Facilities (NSF) country code.
FaxRelayNsfManufCode	Fax relay NSF manufacturers code.
FaxRelayPktLossConceal	Fax relay packet loss conceal.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>dial-control-mib</b>	Specifies attributes for the call history table.
<b>show call active fax</b>	Displays call information for fax transmissions that are in progress.
<b>show call active voice</b>	Displays call information for voice calls that are in progress.
<b>show call history voice</b>	Displays the call history table for voice calls.
<b>show dial-peer voice</b>	Displays configuration information for dial peers.
<b>show num-exp</b>	Displays how the number expansions are configured in VoIP.
<b>show voice port</b>	Displays configuration information about a specific voice port.

# show call history voice

To display the call history table for voice calls, use the **show call history voice** command in user EXEC or privileged EXEC mode.

```
show call history voice [brief [id identifier] | compact [duration {less | more} seconds]
| id identifier | last number | redirect {rtpvt | tbct} | stats]
```

Syntax Description	
<b>brief</b>	(Optional) Displays a truncated version of the call history table.
<b>id identifier</b>	(Optional) Displays only the call with the specified identifier. Range is from 1 to FFFF.
<b>compact</b>	(Optional) Displays a compact version of the call history table.
<b>duration seconds</b>	(Optional) Displays history information for calls that are longer or shorter than the value of the specified <i>seconds</i> argument. The arguments and keywords are as follows: <ul style="list-style-type: none"> <li><b>less</b>—Displays calls shorter than the <i>seconds</i> value.</li> <li><b>more</b>—Displays calls longer than the <i>seconds</i> value.</li> <li><i>seconds</i>—Elapsed time, in seconds. Range is from 1 to 2147483647.</li> </ul>
<b>last number</b>	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the <i>number</i> argument. Range is from 1 to 100.
<b>redirect</b>	(Optional) Displays information about calls that were redirected using Release-to-Pivot (RTPvt) or Two B-Channel Transfer (TBCT). The keywords are as follows: <ul style="list-style-type: none"> <li><b>rtpvt</b>—Displays information about RTPvt calls.</li> <li><b>tbct</b>—Displays information about TBCT calls.</li> </ul>
<b>stats</b>	(Optional) Displays information about digital signal processing (DSP) voice quality metrics.

Command Modes	
	User EXEC (>) Privileged EXEC (#)

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series.
	12.0(3)XG	Support was added for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
	12.0(4)XJ	This command was modified for store-and-forward fax.
	12.0(4)T	The <b>brief</b> keyword was added, and the command was implemented on the Cisco 7200 series.
	12.0(5)XK	This command was implemented on the Cisco MC3810.
	12.0(7)XK	The <b>brief</b> keyword was implemented on the Cisco MC3810.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Release	Modification
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XA	The output of this command was modified to indicate whether a specified call has been established using Annex E.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
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 was not included for the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.2(11)T	Support was added for Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.2(13)T	The ReleaseSource field was added to the Field Description table, and the <b>record</b> keyword was deleted from the command name.
12.3(1)	The <b>redirect</b> keyword was added.
12.4(2)T	The LocalHostname display field was added to the VoIP call leg record.
12.4(11)XW	The <b>stats</b> keyword was added.
12.4(15)T	The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	Command output was updated to show IPv6 information.

### Usage Guidelines

This command displays a call-history table that contains a list of voice calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number from 0 to 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed. The timer value is also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the **last** keyword, and define the number of calls to be displayed with the *number* argument.

To display a truncated version of the call history table, use the **brief** keyword.

Use the **show call active voice redirect** command to review records for calls that implemented RTPvt or TBCT.

When a call is active, you can display its statistics by using the **show call active voice** command.

### Examples

The following is sample output from the **show call history voice** command:

```
Router# show call history voice

GENERIC:
SetupTime=104648 ms
Index=1
PeerAddress=55240
PeerSubAddress=
```

```
PeerId=2
PeerIfIndex=105
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
DisconectTime=143329
CallDuration=00:06:23
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=37668
TransmitBytes=6157536
ReceivePackets=37717
ReceiveBytes=6158452
VOIP:
ConnectionId[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
CallID=2
RemoteIPAddress=10.14.82.14
RemoteUDPPort=18202
RoundTripDelay=2 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE

SessionProtocol=cisco
SessionTarget=ipv4:10.14.82.14
OnTimeRvPlayout=40
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=67 ms
LoWaterPlayoutDelay=67 ms
ReceiveDelay=67 ms
LostPackets=0 ms
EarlyPackets=0 ms
LatePackets=0 ms
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
cvVoIPCallHistoryIcpif=0
SignalingType=cas

Modem passthrough signaling method is nse
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 373sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

GENERIC:
SetupTime=104443 ms
Index=2
PeerAddress=50110
PeerSubAddress=
PeerId=100
PeerIfIndex=104
LogicalIfIndex=10
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
```

■ **show call history voice**

```

DisconnectTime=143330
CallDuration=00:06:23
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=37717
TransmitBytes=5706436
ReceivePackets=37668
ReceiveBytes=6609552
TELE:
ConnectionId=[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
CallID=3
Port=3/0/0 (3)
BearerChannel=3/0/0.1
TxDuration=375300 ms
VoiceTxDuration=375300 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-75
ACOMLevel=11
SessionTarget=
ImgPages=0

```

The following example from a Cisco AS5350 router displays a sample of voice call history records showing release source information:

```

Router# show call history voice

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Total call-legs: 2

GENERIC:
SetupTime=85975291 ms
.
.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975335
DisconnectTime=85979339
CallDuration=00:00:40
CallOrigin=1
ReleaseSource=1
.
.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975335
DisconnectTime=85979339
CallDuration=00:00:40
CallOrigin=1
ReleaseSource=1
.
.
.
VOIP:
ConnectionId[0x2868AD84 0x375B11D4 0x8012F7A5 0x74DE971E]
CallID=1
.
.

```

```

.
GENERIC:
SetupTime=85975290 ms
.
.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975336
DisconnectTime=85979340
CallDuration=00:00:40
CallOrigin=2
ReleaseSource=1
.
.
.
TELE:
ConnectionId=[0x2868AD84 0x375B11D4 0x8012F7A5 0x74DE971E]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1

```

The following is sample output from the **show call history voice brief** command:

```
Router# show call history voice brief
```

```

<ID>: <CallID> <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause> (<text>)
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
Telephony <int> (callID) [channel_id] tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm
acom:<lvl>dBm
MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
disc:<cause code>
speeds (bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>

```

The following is sample output from the **show call history voice redirect** command:

```
Router# show call history voice redirect tbct
```

```

index=2, xfr=tbct-notify, status=redirect_success, start_time=*00:12:25.981 UTC Mon Mar 1
1993, ctrl name=T1-2/0, tag=13
index=3, xfr=tbct-notify, status=redirect_success, start_time=*00:12:25.981 UTC Mon Mar 1
1993, ctrl name=T1-2/0, tag=13
index=4, xfr=tbct-notify, status=redirect_success, start_time=*00:13:07.091 UTC Mon Mar 1
1993, ctrl name=T1-2/0, tag=12
index=5, xfr=tbct-notify, status=redirect_success, start_time=*00:13:07.091 UTC Mon Mar 1
1993, ctrl name=T1-2/0, tag=12

```

```
Number of call-legs redirected using tbct with notify:4
```

Table 139 describes the significant fields shown in the **show call history voice redirect tbct** display.

**Table 139** *show call history voice redirect Field Descriptions*

Field	Description
index	Index number of the record in the history file.
xfr	Whether TBCT or TBCT with notify has been invoked.
status	Status of the redirect request.
start_time	Time, in hours, minutes, and seconds when the redirected call began.
ctrl name	Name of the T1 controller where the call originated.
tag	Call tag number that identifies the call.
Number of call-legs redirected using tbct with notify	Total number of call legs that were redirected using TBCT with notify.

#### Related Commands

Command	Description
<b>dial-control-mib</b>	Set the maximum number of calls contained in the table.
<b>show call active fax</b>	Displays call information for fax transmissions that are in progress.
<b>show call active voice</b>	Displays call information for voice calls that are in progress.
<b>show call history fax</b>	Displays the call history table for fax transmissions.
<b>show dial-peer voice</b>	Displays configuration information for dial peers.
<b>show num-exp</b>	Displays how the number expansions are configured in VoIP.
<b>show voice port</b>	Displays configuration information about a specific voice port.

# show cdp entry

To display information about a specific neighboring device discovered using Cisco Discovery Protocol (CDP), use the **show cdp entry** command in privileged EXEC mode.

```
show cdp entry {* | device-name[*]} [version] [protocol]
```

## Syntax Description

<b>*</b>	Displays all of the CDP neighbors.
<i>device-name</i> [*]	Name of the neighbor about which you want information. You can enter an optional asterisk (*) at the end of a <i>device-name</i> as a wildcard. For example, entering <b>show cdp entry dev*</b> will match all device names that begin with <b>dev</b> .
<b>version</b>	(Optional) Limits the display to information about the version of software running on the router.
<b>protocol</b>	(Optional) Limits the display to information about the protocols enabled on a router.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
10.3	This command was introduced.
12.2(8)T	Support for IPv6 address and address type information was 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(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.
12.2SX	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 cdp entry** command. Information about the neighbor *device.cisco.com* is displayed, including device ID, protocols and addresses, platform, interface, hold time, and version.

```
Router# show cdp entry device.cisco.com

Device ID: device.cisco.com
Entry address(es):
  IP address: 10.1.17.24
  IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06 (global unicast)
  CLNS address: 490001.1111.1111.1111.00
Platform: cisco 3640, Capabilities: Router
Interface: Ethernet0/1, Port ID (outgoing port): Ethernet0/1
Holdtime : 160 sec

Version :
```

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 08-Aug-01 12:39 by joeuser
```

Table 140 describes the significant fields shown in the example.

**Table 140** *show cdp entry Field Descriptions*

Field	Definition
Device ID: device.cisco.com	Name or ID of the device.
Entry address(es):	The IP, IPv6 link-local, IPv6 global unicast, and CLNS addresses.
Platform:	Platform information specific to the device.
Interface: Ethernet0/1, Port ID (outgoing port): Ethernet0/1	Information about the interface and port ID interface.
Holdtime:	Holdtime length in seconds.
Version:	Information about the software version.

The following is sample output from the **show cdp entry version** command. Only information about the version of software running on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com version

Version information for device.cisco.com:
 Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 08-Aug-01 12:39 by joeuser
```

The following is sample output from the **show cdp entry protocol** command. Only information about the protocols enabled on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com protocol

Protocol information for device.cisco.com:
 IP address: 10.1.17.24
 IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local)
 IPv6 address: 4000::BC:0:0:C0A8:BC06 (global unicast)
 CLNS address: 490001.1111.1111.1111.00
```

## Related Commands

Command	Description
<b>show cdp</b>	Displays global CDP information, including timer and hold-time information.
<b>show cdp interface</b>	Displays information about the interfaces on which CDP is enabled.
<b>show cdp neighbors</b>	Displays detailed information about neighboring devices discovered using CDP.
<b>show cdp traffic</b>	Displays traffic information from the CDP table.

# show cdp neighbors

To display detailed information about neighboring devices discovered using Cisco Discovery Protocol, use the **show cdp neighbors** command in privileged EXEC mode.

**show cdp neighbors** [*type number*] [**detail**]

## Syntax Description

<i>type</i>	(Optional) Interface type that is connected to the neighbors about which you want information; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>port-channel</b> , and <b>vlan</b> .
<i>number</i>	(Optional) Number of the interface connected to the neighbors about which you want information.
<b>detail</b>	(Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	The output of this command using the <b>detail</b> keyword was expanded to include Cisco Discovery Protocol Version 2 information.
12.2(8)T	Support for IPv6 address and address type information was added.
12.2(14)S	Support for IPv6 address and address type information was added.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
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.
12.2SX	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.

## Usage Guidelines

The **vlan** keyword is supported in Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **port-channel** values are from 0 to 282; values from 257 to 282 are supported on the call switching module (CSM) and the firewall services module (FWSM) only.

## Examples

The following is sample output from the **show cdp neighbors** command:

```
Router# show cdp neighbors
```

```
Capability Codes:R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch,
```

```

H - Host, I - IGMP, r - Repeater
Device ID Local Intrfce Holdtme Capability Platform Port ID
joe       Eth 0         133      R          4500      Eth 0
sam       Eth 0         152      R          AS5200    Eth 0
terri     Eth 0         144      R          3640      Eth0/0
maine     Eth 0         141      R          RP1        Eth 0/0
sancho    Eth 0         164      R          7206      Eth 1/0

```

Table 140 describes the fields shown in the display.

**Table 141** *show cdp neighbors Field Descriptions*

Field	Definition
Capability Codes	The type of device that can be discovered.
Device ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Local Intrfce	The local interface through which this neighbor is connected.
Holdtme	The remaining amount of time (in seconds) the current device will hold the Cisco Discovery Protocol advertisement from a sending router before discarding it.
Capability	The type of the device listed in the CDP Neighbors table. Possible values are as follows: <ul style="list-style-type: none"> <li>• R—Router</li> <li>• T—Transparent bridge</li> <li>• B—Source-routing bridge</li> <li>• S—Switch</li> <li>• H—Host</li> <li>• I—IGMP device</li> <li>• r—Repeater</li> </ul>
Platform	The product number of the device.
Port ID	The interface and port number of the neighboring device.

The following is sample output for one neighbor from the **show cdp neighbors detail** command. Additional detail is shown about neighbors, including network addresses, enabled protocols, and software version.

```

Router# show cdp neighbors detail

Device ID: device.cisco.com
Entry address(es):
  IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local)
  IPv6 address: 4000::BC:0:0:COA8:BC06 (global unicast)
Platform: cisco 3640, Capabilities: Router
Interface: Ethernet0/1, Port ID (outgoing port): Ethernet0/1
Holdtime : 160 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Version 12.2(25)SEB4, RELE)
advertisement version: 2
Duplex Mode: half
Native VLAN: 42

```

VTP Management Domain: 'Accounting Group'

Table 142 describes the fields shown in the display.

**Table 142** *show cdp neighbors detail Field Descriptions*

Field	Definition
Device ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Entry address(es)	A list of network addresses of neighbor devices.
IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local)	<p>The network address of the neighbor device. The address can be in IP, IPv6, IPX, AppleTalk, DECnet, or Connectionless Network Service (CLNS) protocol conventions.</p> <p>IPv6 addresses are followed by one of the following IPv6 address types:</p> <ul style="list-style-type: none"> <li>• global unicast</li> <li>• link-local</li> <li>• multicast</li> <li>• site-local</li> <li>• V4 compatible</li> </ul> <p><b>Note</b> For Cisco IOS Releases 12.2(33)SXH3, Release 12.2(33)SXI and later releases, the command will not display the AppleTalk address.</p>
Platform	The product name and number of the neighbor device.
Capabilities	The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
Interface	The local interface through which this neighbor is connected.
Port ID	The interface and port number of the neighboring device.
Holdtime	The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending router before discarding it.
Version	The software version of the neighbor device.
advertisement version:	Version of CDP that is being used for CDP advertisements.
Duplex Mode	The duplex state of connection between the current device and the neighbor device.
Native VLAN	The ID number of the VLAN on the neighbor device.
VTP Management Domain	A string that is the name of the collective group of VLANs associated with the neighbor device.

## ■ show cdp neighbors

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show cdp</b>	Displays global CDP information, including timer and hold-time information.
<b>show cdp entry</b>	Displays information about a specific neighbor device listed in the CDP table.
<b>show cdp interface</b>	Displays information about the interfaces on which CDP is enabled.
<b>show cdp traffic</b>	Displays information about traffic between devices gathered using CDP.

# show cef

To display information about packets forwarded by Cisco Express Forwarding, use the **show cef** command in privileged EXEC mode.

```
show cef { accounting | background [detail] | broker broker-name [detail] | error | fib |
hardware vectors | idb | loadinfo | non-ip | nsf | path [list [walk] | sets [detail | id path-set-id
| summary] | switching background [detail] | walks [process | queue]}
```

Syntax	Description
<b>accounting</b>	Displays Cisco Express Forwarding accounting state.
<b>background</b>	Displays Cisco Express Forwarding background processing.
<b>detail</b>	(Optional) Displays detailed Cisco Express Forwarding information.
<b>broker</b> <i>broker-name</i>	(Distributed platforms only) Displays Cisco Express Forwarding information related to update brokers.
<b>error</b>	Displays information about the state of Cisco Express Forwarding errors.
<b>fib</b>	Displays Cisco Express Forwarding Forwarding Information Base (FIB) entries.
<b>hardware vectors</b>	Displays the hardware application programming interface (API) vector function table.
<b>idb</b>	Displays Cisco Express Forwarding interface descriptor blocks.
<b>loadinfo</b>	Displays Cisco Express Forwarding loadinfo events.
<b>non-ip</b>	Displays Cisco Express Forwarding paths for non-IP traffic.
<b>nsf</b>	(Distributed platforms only) Displays Cisco Express Forwarding nonstop forwarding (NSF) statistics.
<b>path</b>	Displays Cisco Express Forwarding paths.
<b>list</b>	(Optional) Displays a list of Cisco Express Forwarding paths.
<b>walk</b>	(Optional) Displays the walk through the list of Cisco Express Forwarding paths.
<b>sets</b>	(Optional) Displays point-to-multipoint path set information.
<b>detail</b>	(Optional) Displays detailed point-to-multipoint path set information.
<b>id</b> <i>path-set-id</i>	(Optional) Displays information about the specified path set. Enter the path set ID in hex format.
<b>summary</b>	(Optional) Displays high-level information about point-to-multipoint path sets.
<b>switching background</b>	Display Cisco Express Forwarding background switching processing.
<b>walks</b>	Specifies a walk through Cisco Express Forwarding infrastructure.
<b>process</b>	(Optional) Displays the process that services the background work queue.
<b>queue</b>	(Optional) Displays the work queue of background walks.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	11.2GS	This command was introduced to support the Cisco 12012 Internet router.
	11.1CC	Support was added for multiple platforms.
	12.0(22)S	The display output for this command was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 packets.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(25)S	The <b>drop</b> and <b>not-cef-switched</b> keywords were removed. The <b>accounting</b> , <b>background</b> , <b>broker</b> , <b>fib</b> , <b>hardware vectors</b> , <b>idb</b> , <b>loadinfo</b> , <b>non-ip</b> , <b>nsf</b> , <b>path</b> , and <b>walks</b> keywords were 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(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.
	12.2(33)SRE	This command was modified. The <b>sets</b> keyword was added to display point-to-multipoint information.

### Usage Guidelines

Use this command to display and monitor information about traffic forwarded by Cisco Express Forwarding.

A line card might drop packets because of encapsulation failure, absence of route information, or absence of adjacency information.

A packet is punted (sent to another switch path) because Cisco Express Forwarding may not support a specified encapsulation or feature, the packet may be destined for the router, or the packet may have IP options (such as time stamp and record route). IP options are process switched.

### Examples

The following example shows how to display Cisco Express Forwarding accounting information:

```
Router# show cef accounting

IPv4 accounting state:
  Enabled accounting:          per-prefix, non-recursive, prefix-length
  Non-recursive load interval: 30 (default 30)
  Non-recursive update interval: 0 (default 0)

IPv6 accounting state:
  Enabled accounting:          None
  Non-recursive load interval: 30 (default 30)
  Non-recursive update interval: 0 (default 0)
```

[Table 143](#) describes the significant fields shown in the example.

**Table 143** *show cef accounting Field Descriptions*

Field	Description
Enabled accounting	Type or types of Cisco Express Forwarding accounting that are enabled: load-balance-hash, non-recursive, per-prefix, prefix-length, or none.
per-prefix	Indicates that Cisco Express Forwarding accounting is enabled for the collection of the number of packets and bytes express-forwarded to a destination (or prefix).
non-recursive	Indicates that Cisco Express Forwarding accounting is enabled through nonrecursive prefixes.
prefix-length	Indicates that Cisco Express Forwarding accounting is enabled through prefix length.

The following example shows how to display Cisco Express Forwarding background information:

```
Router# show cef background
```

```
CEF background process process (pid 77) running
 0 events awaiting registration on background process
 9 events registered on background process
  boolean   FIB malloc failed, 0 occurrences
  boolean   FIB assert failed, 0 occurrences
  boolean   FIB hw_api_failure failed, 0 occurrences
  timer     FIB checkers: auto-repair delay, init, !run, 0 occurrences
  timer     FIB checkers: auto-repair delay, init, !run, 0 occurrences
  timer     FIB checkers: IPv4 scan-rib-ios scanner, init, run, 2 occurrences
  timer     FIB checkers: IPv4 scan-ios-rib scanner, init, run, 2 occurrences
  timer     FIB checkers: IPv6 scan-ios-rib scanner, init, run, 2 occurrences
  timer     FIB table: rate monitor, init, run, 0 occurrences
```

Table 144 describes the significant fields shown in the example.

**Table 144** *show cef background Field Descriptions*

Field	Description
boolean	The background process is waiting for a true or false flag to be set.
FIB malloc failed, 0 occurrences	No instances of memory allocation failure have occurred for the FIB.
FIB assert failed, 0 occurrences	No instances of assertion failure have occurred for the FIB.
FIB hw_api_failure failed; 0 occurrences	No failures are reported during the programming of hardware forwarding.
timer	The background process is waiting for a timer to be triggered. Once the timer is triggered, the operation begins. In the FIB checkers cases that follow, the timer is linked to Cisco Express Forwarding consistency checkers.
FIB checkers: auto-repair delay, init, !run, 0 occurrences	FIB auto repair timer is initialized, but the timer is not running and has not been running (0 occurrences).
FIB checkers: IPv4 scan-rib-ios scanner, init, !run, 2 occurrences	FIB IPv4 scan-rib-ios timer is initialized and running. The timer has been triggered twice.

**Table 144** *show cef background Field Descriptions*

Field	Description
FIB checkers: IPv4 scan-ios-rib scanner, init, run, 2 occurrences	FIB IPv4 scan-ios-rib timer is initialized and running. The timer has been triggered twice.
FIB table: rate monitor, init, run, 0 occurrences	FIB table rate monitor timer is initialized and running, but has yet to be triggered.

The following example shows how to display information about Cisco Express Forwarding FIB entries:

```
Router# show cef fib

9 allocated IPv4 entries, 0 failed allocations
1 allocated IPv6 entry, 0 failed allocations
```

Table 145 describes the significant fields shown in the example.

**Table 145** *show cef fib Field Descriptions*

Field	Description
9 allocated IPv4 entries, 0 failed allocations	Number of successfully allocated and failed IPv4 entries.
1 allocated IPv6 entry, 0 failed allocations	Number of successfully allocated and failed IPv6 entries.

The following example shows how to display information about Cisco Express Forwarding loadinfo:

```
Router# show cef loadinfo

0 allocated loadinfos, 0 failed allocations
0 allocated loadinfo hash usage gsbs
0 inplace modifies (enabled)
0 identical modifies
```

Table 146 describes the significant fields shown in the example.

**Table 146** *show cef loadinfo Field Descriptions*

Field	Description
0 allocated loadinfos, 0 failed allocations	Number of successfully allocated and failed allocated loadinfos.
0 allocated loadinfo hash usage gsbs	Number of allocated subblocks for per-hash bucket accounting when load balancing is used.
0 inplace modifies (enabled)	In-place modification is enabled. No in-place modifications have occurred.
0 identical modifies	Number of in-place modifications that were skipped because the replacement was identical to the target.

The following example shows how to display information for Cisco Express Forwarding paths:

```
Router# show cef path

28 allocated IPv4 paths, 0 failed allocations
4 allocated IPv6 paths, 0 failed allocations
```

32 Total Paths, 587 Recursive Paths, 0 Unresolved Paths

Table 147 describes the significant fields shown in the example.

**Table 147** *show cef path Field Descriptions*

Field	Definition
28 allocated IPv4 paths	Number of successfully allocated and failed IPv4 paths.
4 allocated IPv6 paths	Number of successfully allocated and failed IPv6 paths.
32 Total Paths, 587 Recursive Paths, 0 Unresolved Paths	Information on all Cisco Express Forwarding paths.

The following example shows how to display information about Cisco Express Forwarding background switching processes:

```
Router# show cef switching background

CEF switching background process (pid 46) running
 0 events awaiting registration on background process
 1 event registered on background process
 boolean   OCE unlock queue, 0 occurrences
```

Table 148 describes the significant fields shown in the example.

**Table 148** *show cef switching background Field Descriptions*

Field	Description
0 events awaiting registration on background process	Number of events waiting to be registered on the background process.
1 event registered on background process	Number of events registered on the background process.
boolean   OCE unlock queue, 0 occurrences	Number of output chain element (OCE) unlock queue events.

The following example shows how to display information about Cisco Express Forwarding:

```
Router# show cef walks

Calling process:
-----

Number of initial walks:

mode / priority      started
                    low      high   very high
sync                 3          0         0
atomic               0          0         0

mode / priority      finished
                    low      high   very high
sync                 3          0         0
atomic               0          0         0

mode / priority      restarted
                    low      high   very high
```

```

sync                0                0                0
atomic              0                0                0

Number of sub walks:

mode / priority      started
                    low          high         very high
sync                0                0                0
atomic              0                0                0

mode / priority      finished
                    low          high         very high
sync                0                0                0
atomic              0                0                0

```

Table 149 describes the significant fields shown in the example.

**Table 149** *show cef walks Field Description*

Field	Description
mode	Indicates the mode of the Cisco Express Forwarding infrastructure walk: <ul style="list-style-type: none"> <li>• sync—The walk takes place in the current process context and completes before the start function returns. Other processes are allowed to run.</li> <li>• atomic—The walk takes place in the current process context and completes before the start function returns. No other processes are allowed to run.</li> </ul>
priority	Indicate the priority of the infrastructure walk: low, medium, or high.

#### Related Commands

Command	Description
<b>clear cef linecard</b>	Clears Cisco Express Forwarding information from line cards.
<b>show cef features global</b>	Displays Cisco Express Forwarding features for any interface.
<b>show cef interface</b>	Displays detailed Cisco Express Forwarding information for a specified interface or for all interfaces.
<b>show cef linecard</b>	Displays Cisco Express Forwarding-related information by line card.
<b>show cef memory</b>	Displays information about Cisco Express Forwarding memory usage.
<b>show cef state</b>	Displays the state of Cisco Express Forwarding on a networking device.
<b>show cef subtree context client</b>	Displays Cisco Express Forwarding prefix subtrees.
<b>show cef table</b>	Displays the configuration and operational state of the Cisco Express Forwarding FIB table.
<b>show cef timers</b>	Displays the current state of the timers internal to the Cisco Express Forwarding process.

# show cef interface

To display detailed Cisco Express Forwarding information for a specified interface or for all interfaces, use the **show cef interface** command in user EXEC or privileged EXEC mode.

```
show cef interface [type number] [statistics | detail | internal | brief | policy-statistics [input | output]]
```

Syntax Description	
<i>type number</i>	(Optional) Interface type and number. No space is required between the interface type and number.
<b>statistics</b>	(Optional) Displays switching statistics for an interface or interfaces.
<b>detail</b>	(Optional) Displays detailed Cisco Express Forwarding information for the specified interface type and number.
<b>internal</b>	(Optional) Displays internal Cisco Express Forwarding interface status and configuration.
<b>brief</b>	(Optional) Summarizes the Cisco Express Forwarding interface state.
<b>policy-statistics</b>	(Optional) Displays Border Gateway Protocol (BGP) policy statistical information for a specific interface or for all interfaces.
<b>input</b>	(Optional) Displays BGP accounting policy statistics for traffic that is traveling through an input interface.
<b>output</b>	(Optional) Displays BGP accounting policy statistics for traffic that is traveling through an output interface.

Command Modes	
	User EXEC (>)
	Privileged EXEC (#)

Command History	Release	Modification
	11.2GS	This command was introduced to support the Cisco 12012 Internet router.
	11.1CC	Support for multiple platforms was added.
	12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST, and the <b>statistics</b> keyword was added.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T, and the <b>detail</b> keyword was added.
	12.2(13)T	The <b>policy-statistics</b> keyword was added.
	12.0(22)S	The <b>input</b> and <b>output</b> keywords were added.
		The display output was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding interface information. Output fields that support BGP policy accounting were added for the Cisco 7200 series and Cisco 7500 series platforms.

Release	Modification
12.3(4)T	The <b>input</b> and <b>output</b> keywords were added.  The display output was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding interface information. Output fields that support BGP policy accounting were added for the Cisco 7200 series and Cisco 7500 series platforms.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The <b>internal</b> 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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

### Usage Guidelines

You can use this command to display the detailed Cisco Express Forwarding status for all interfaces. Values entered for the *type* and *number* arguments display Cisco Express Forwarding status information for the specified interface type and number.

The **policy-statistics**, **input**, and **output** keywords are available only on distributed switching platforms.

### Examples

The following example shows how to display a summary of Cisco Express Forwarding information for an interface named Ethernet 3/0:

```
Router# show cef interface ethernet 3/0 brief

Interface                IP-Address      Status  Switching
Ethernet3/0              10.0.212.6     up      CEF
Router#
```

The following is sample output from the **show cef interface** command for Fast Ethernet interface 1/0/0 with BGP policy accounting configured for input traffic:

```
Router# show cef interface fastethernet 1/0/0

FastEthernet1/0/0 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  Internet address is 10.1.1.1/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  BGP based policy accounting on input is enabled
  BGP based policy accounting on output is disabled
Hardware idb is FastEthernet1/0/0 (6)
Software idb is FastEthernet1/0/0 (6)
Fast switching type 1, interface type 18
IP Distributed CEF switching enabled
IP Feature Fast switching turbo vector
IP Feature CEF switching turbo vector
Input fast flags 0x100, Output fast flags 0x0, Flags 0x0
```

```
ifindex 7(7)
Slot 1 Slot unit 0 VC -1
Transmit limit accumulator 0xE8001A82 (0xE8001A82)
IP MTU 1500
```

The following is sample output from the **show cef interface detail** command for Ethernet interface 1/0/0:

```
Router# show cef interface ethernet 1/0/0 detail

FastEthernet1/0/0 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  Internet address is 10.1.1.1/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  BGP based policy accounting on input is enabled
  BGP based policy accounting on output is disabled
  Hardware idb is FastEthernet1/0/0 (6)
  Software idb is FastEthernet1/0/0 (6)
  Fast switching type 1, interface type 18
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x100, Output fast flags 0x0, Flags 0x0
  ifindex 7(7)
  Slot 1 Slot unit 0 VC -1
  Transmit limit accumulator 0xE8001A82 (0xE8001A82)
  IP MTU 1500
```

The following is sample output from the **show cef interface Null 0 detail** command:

```
Router# show cef interface null 0 detail

Null0 is up (if_number 1)
  Corresponding hwidb fast_if_number 1
  Corresponding hwidb firstsw->if_number 1
  Internet Protocol processing disabled
  Interface is marked as nullidb
  Packets switched to this interface on linecard are dropped to next slow path
  Hardware idb is Null0
  Fast switching type 13, interface type 0
  IP CEF switching enabled
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 0(0)
  Slot -1 Slot unit -1 VC -1
  Transmit limit accumulator 0x0 (0x0)
  IP MTU 1500
```

The following is sample output for internal Cisco Express Forwarding interface status and configuration for the Ethernet 3/1 interface:

```
Router# show cef interface ethernet 3/1 internal

Ethernet3/1 is up (if_number 13)
  Corresponding hwidb fast_if_number 13
  Corresponding hwidb firstsw->if_number 13
  Internet address is 10.0.212.6/24
  ICMP redirects are always sent
```

```

Per packet load-sharing is disabled
IP unicast RPF check is disabled
Inbound access list is not set
Outbound access list is not set
IP policy routing is disabled
BGP based policy accounting on input is disabled
BGP based policy accounting on output is disabled
Hardware idb is Ethernet3/1
Fast switching type 1, interface type 63
IP CEF switching enabled
IP CEF switching turbo vector
IP CEF turbo switching turbo vector
IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
Input fast flags 0x0, Output fast flags 0x0
ifindex 11(11)
Slot 3 Slot unit 0 VC -1
Transmit limit accumulator 0x0 (0x0)
IP MTU 1500
Subblocks:
IPv6: enabled 1 unreachable FALSE redirect TRUE mtu 1500 flags 0x0
      link-local address is FE80::20C:CFFF:FEF9:4854
      Global unicast address(es):
      10:6:6:6:20C:CFFF:FEF9:4854, subnet is 10:6:6:6::/64 [EUI]
IPv4: Internet address is 10.0.212.6/24
      Broadcast address 255.255.255.255
      Per packet load-sharing is disabled
      IP MTU 1500

```

Table 150 describes the significant fields shown in the displays.

**Table 150 show cef interface Field Descriptions**

Field	Description
FastEthernet1/0/0 is up	Indicates type, number, and status of the interface.
Internet address is	Internet address of the interface.
ICMP redirects are always sent	Indicates how packet forwarding is configured.
Per packet load-sharing is disabled	Indicates status of load sharing on the interface.
IP unicast RPF check is disabled	Indicates status of IP unicast Reverse Path Forwarding (RPF) check on the interface.
Inbound access list is not set	Indicates the number or name of the inbound access list if one is applied to this interface. Also indicates whether the list is set.
Outbound access list is not set	Indicates the number or name of the outbound access list if one is applied to this interface. Also indicates whether the list is set.
IP policy routing is disabled	Indicates the status of IP policy routing on the interface.
BGP based policy accounting on input is enabled	Indicates the status of BGP policy accounting on the input interface.
BGP based policy accounting on output is disabled	Indicates the status of BGP policy accounting on the output interface.
Hardware idb is Ethernet1/0/0	Interface type and number configured.

**Table 150** show cef interface Field Descriptions (continued)

Field	Description
Fast switching type	Used for troubleshooting; indicates switching mode in use.
Interface type	Indicates interface type.
IP Distributed CEF switching enabled	Indicates whether distributed Cisco Express Forwarding is enabled on this interface. (Cisco 7500 and 12000 series Internet routers only.)
IP Feature Fast switching turbo vector	Indicates IP fast switching type configured.
IP Feature CEF switching turbo vector	Indicates IP feature Cisco Express Forwarding switching type configured.
Input fast flags	Indicates the input status of various switching features: <ul style="list-style-type: none"> <li>• 0x0001 (input Access Control List [ACL] enabled)</li> <li>• 0x0002 (policy routing enabled)</li> <li>• 0x0004 (input rate limiting)</li> <li>• 0x0008 (MAC/Prec accounting)</li> <li>• 0x0010 (DSCP/PREC/QOS GROUP)</li> <li>• 0x0020 (input named access lists)</li> <li>• 0x0040 (NAT enabled on input)</li> <li>• 0x0080 (crypto map on input)</li> <li>• 0x0100 (QPPB classification)</li> <li>• 0x0200 (inspect on input)</li> <li>• 0x0400 (input classification)</li> <li>• 0x0800 (<sup>1</sup>casa input enable)</li> <li>• 0x1000 (Virtual Private Network [VPN] enabled on a <sup>2</sup>swidb)</li> <li>• 0x2000 (input idle timer enabled)</li> <li>• 0x4000 (unicast Reverse Path Forwarding [RPF] check)</li> <li>• 0x8000 (per-address ACL enabled)</li> <li>• 0x10000 (deaggregating a packet)</li> <li>• 0x20000 (<sup>3</sup>GPRS enabled on input)</li> <li>• 0x40000 (URL RenDezvous)</li> <li>• 0x80000 (QoS classification)</li> <li>• 0x100000 (FR switching on interface)</li> <li>• 0x200000 (<sup>4</sup>WCCP redirect on input)</li> <li>• 0x400000 (input classification)</li> </ul>

**Table 150** show cef interface Field Descriptions (continued)

Field	Description
Output fast flags	Indicates the output status of various switching features, as follows: <ul style="list-style-type: none"> <li>• 0x0001 (output ACL enabled)</li> <li>• 0x0002 (IP accounting enabled)</li> <li>• 0x0004 (WCC redirect enabled interface)</li> <li>• 0x0008 (rate limiting)</li> <li>• 0x0010 (MAC/Prec accounting)</li> <li>• 0x0020 (DSCP/PREC/QOS GROUP)</li> <li>• 0x0040 (D-QOS classification)</li> <li>• 0x0080 (output named access lists)</li> <li>• 0x0100 (NAT enabled on output)</li> <li>• 0x0200 (TCP intercept enabled)</li> <li>• 0x0400 (crypto map set on output)</li> <li>• 0x0800 (output firewall)</li> <li>• 0x1000 (<sup>5</sup>RSVP classification)</li> <li>• 0x2000 (inspect on output)</li> <li>• 0x4000 (QoS classification)</li> <li>• 0x8000 (QoS preclassification)</li> <li>• 0x10000 (output stile)</li> </ul>
ifindex 7/(7)	Indicates a Cisco IOS internal index or identifier for this interface.
Slot 1 Slot unit 0 VC -1	The slot number and slot unit.
Transmit limit accumulator	Indicates the maximum number of packets allowed in the transmit queue.
IP MTU	The MTU size set on the interface.

1. Cisco applications and services architecture (CASA)
2. Software interface descriptor block (SWIDB)
3. General packet radio system (GPRS)
4. Web cache communication protocol (WCCP)
5. Resource reservation protocol (RSVP)

The following is sample output from the **show cef interface command** using the **policy-statistics** keyword:

```
Router# show cef interface policy-statistics
```

```
POS7/0 is up (if_number 8)
Index  Packets          Bytes
-----  -----
1           0                0
2           0                0
3          50             5000
```

4	100	10000
5	100	10000
6	10	1000
7	0	0
8	0	0

The following is sample output from the **show cef interface** command using the **policy-statistics** keyword. It shows policy statistics for Ethernet interface 1/0.

```
Router# show cef interface ethernet 1/0 policy-statistics
```

```
Ethernet1/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
Index          Packets          Bytes
  1              0              0
  2              0              0
  3              0              0
  4              0              0
  5              0              0
  6              0              0
  7              0              0
  8              0              0
```

The following is sample output from the **show cef interface** command using the **policy-statistics** keyword. It shows policy statistics for Fast Ethernet interface 1/0/0 with the policy accounting based on input traffic.

```
Router# show cef interface fastethernet 1/0/0 policy-statistics input
```

```
FastEthernet1/0/0 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  BGP based Policy accounting on input is enabled
Index          Packets          Bytes
  1            9999          999900
  2              0              0
  3              0              0
  4              0              0
  5              0              0
  6              0              0
  7              0              0
  8              0              0
  9              0              0
 10              0              0
 11              0              0
 12              0              0
 13              0              0
 14              0              0
 15              0              0
 16              0              0
 17              0              0
 18              0              0
 19              0              0
 20              0              0
 21              0              0
 22              0              0
 23              0              0
 24              0              0
 25              0              0
 26              0              0
 27              0              0
 28              0              0
 29              0              0
```

■ **show cef interface**

30	0	0
31	0	0
32	0	0
33	0	0
34	1234	123400
35	0	0
36	0	0
37	0	0
38	0	0
39	0	0
40	0	0
41	0	0
42	0	0
43	0	0
44	0	0
45	1000	100000
46	0	0
47	0	0
48	0	0
49	0	0
50	0	0
51	0	0
52	0	0
53	0	0
54	5123	1198782

The following is sample output from the **show cef interface** command using the **policy-statistics** keyword. It shows policy statistics for serial interface 1/1/2 with the policy accounting based on output traffic.

Router# **show cef interface serial 1/1/2 policy-statistics output**

```
Serial1/1/2 is up (if_number 9)
  Corresponding hwidb fast_if_number 9
  Corresponding hwidb firstsw->if_number 9
  BGP based Policy accounting on output is enabled
```

Index	Packets	Bytes
1	9999	999900
2	0	0
.		
.		
.		
18	0	0
19	0	0
20	0	0
.		
.		
.		
34	1234	123400
35	0	0
.		
.		
.		
44	0	0
45	1000	100000
46	0	0
47	0	0
48	0	0
49	0	0
50	0	0
51	0	0
52	0	0
53	0	0
54	5123	1198782

55	0	0
56	0	0
57	0	0
58	0	0
59	0	0
60	0	0
61	0	0
62	0	0
63	0	0
64	0	0

Table 151 describes the significant fields shown in the display.

**Table 151** *show cef interface policy-statistics Field Descriptions*

Field	Description
Index	Traffic index set with the <b>route-map</b> command.
Packets	Number of packets switched that match the index definition.
Bytes	Number of bytes switched that match the index definition.

#### Related Commands

Command	Description
<b>clear cef linecard</b>	Clears Cisco Express Forwarding information from line cards.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
<b>show cef</b>	Displays information about packets forwarded by Cisco Express Forwarding.
<b>show cef drop</b>	Displays which packets the line cards dropped, or displays which packets were not express forwarded.
<b>show cef linecard</b>	Displays Cisco Express Forwarding interface information by line card.

# show cef linecard

To display Cisco Express Forwarding-related information by line card, use the **show cef linecard** command in user EXEC or privileged EXEC mode.

**show cef linecard** [*slot-number*] [**detail**] [**internal**]

Syntax Description		
	<i>slot-number</i>	(Optional) Slot number for the line card about which to display Cisco Express Forwarding-related information. When you omit this argument, information about all line cards is displayed.
	<b>detail</b>	(Optional) Displays detailed Cisco Express Forwarding information for the specified line card.
	<b>internal</b>	(Optional) Displays internal Cisco Express Forwarding information for the specified line card.

Command Modes	
	User EXEC (>)
	Privileged EXEC (#)

Command History	Release	Modification
	11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
	11.1 CC	Multiple platform support was added.
	12.0(10)S	Output display was changed.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and the display output was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 line card information.
	12.2(13)T	The display output modifications made in Cisco IOS Release 12.0(22)S were integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(25)S	The <b>events</b> keyword was removed.
	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.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

**Usage Guidelines** This command is available only on distributed switching platforms.

When you omit the *slot-number* argument, information about all line cards is displayed. When you omit the *slot-number* argument and include the **detail** keyword, detailed information is displayed for all line cards. When you omit the *slot-number* argument and include the **internal** keyword, detailed internal information is displayed for all line cards. When you omit all keywords and arguments, the **show cef linecard** command displays important information about all line cards in table format.

**Examples**

The following is sample output from the **show cef linecard** command. The command displays information for all line cards in table format.

```
Router# show cef linecard

Slot    MsgSent    XDRSent    Window    LowQ    MedQ    HighQ    Flags
0        6           95         24        0       0       0       up
1        6           95         24        0       0       0       up
VRF Default-table, version 8, 6 routes
Slot Version    CEF-XDR    I/Fs State    Flags
0        7           4          8 Active    up, sync
1        7           4          10 Active   up, sync
```

The following is sample output from the **show cef linecard detail** command for all line cards:

```
Router# show cef linecard detail

CEF linecard slot number 0, status up
Sequence number 4, Maximum sequence number expected 28, Seq Epoch 2
Send failed 0, Out Of Sequence 0, drops 0
Linecard CEF reset 0, reloaded 1
95 elements packed in 6 messages(3588 bytes) sent
69 elements cleared
linecard in sync after reloading
0/0/0 xdr elements in LowQ/MediumQ/HighQ
11/9/69 peak elements on LowQ/MediumQ/HighQ
Input  packets 0, bytes 0
Output packets 0, bytes 0, drops 0
CEF Table statistics:
Table name          Version Prefix-xdr Status
Default-table          7          4 Active, up, sync
CEF linecard slot number 1, status up
Sequence number 4, Maximum sequence number expected 28, Seq Epoch 2
Send failed 0, Out Of Sequence 0, drops 0
Linecard CEF reset 0, reloaded 1
95 elements packed in 6 messages(3588 bytes) sent
69 elements cleared
linecard in sync after reloading
0/0/0 xdr elements in LowQ/MediumQ/HighQ
11/9/69 peak elements on LowQ/MediumQ/HighQ
Input  packets 0, bytes 0
Output packets 0, bytes 0, drops 0
CEF Table statistics:
Table name          Version Prefix-xdr Status
Default-table          7          4 Active, up, sync
```

The following is sample output from the **show cef linecard internal** command for all line cards:

```
Router# show cef linecard internal

CEF linecard slot number 0, status up
Sequence number 11, Maximum sequence number expected 35
Send failed 0, Out Of Sequence 0
Linecard CEF reset 2, reloaded 2
Total elements queued:
prefix                4
adjacency             4
interface             91
address               2
policy routing        2
hw interface          57
state                 6
resequence            2
control               13
```

```

table                2
time                4484
flow features deactivate 2
flow cache config   2
flow export config  2
dss                 2
isl                 2
mpls atm vc remove  2
mpls atm vc set label 2
                    2
                    2
                    3
                    1
4574 elements packed in 4495 messages(90286 bytes) sent
115 elements cleared
Total elements cleared:
prefix              2
adjacency           1
interface           63
address             1
policy routing      1
hw interface        29
state               2
control             5
table               1
flow features deactivate 1
flow cache config   1
flow export config  1
dss                 1
isl                 1
mpls atm vc remove  1
mpls atm vc set label 1
                    1
                    1
                    1
linecard disabled - failed a reload
0/0/0 xdr elements in LowQ/MediumQ/HighQ
Input packets 0, bytes 0
Output packets 0, bytes 0, drops 0

CEF Table statistics:
Table name          Version Prefix-xdr Status
Default-table      8           4 Active, sync

```

Table 152 describes the significant fields shown in the displays.

**Table 152** show cef linecard Field Descriptions

Field	Description
Table name	Name of the Cisco Express Forwarding table.
Version	Number of the Forwarding Information Base (FIB) table version.
Prefix-xdr	Number of prefix IPC information elements external data representation (XDRs) processed.
Status	State of the Cisco Express Forwarding table.
Slot	Slot number of the line card.
MsgSent	Number of interprocess communications (IPC) messages sent.
XDRSent	XDRs packed into IPC messages sent from the Route Processor (RP) to the line card.

**Table 152** *show cef linecard Field Descriptions (continued)*

Field	Description
Window	Size of the IPC window between the line card and the RP.
LowQ/MedQ/HighQ	Number of XDR elements in the Low, Medium, and High priority queues.
Flags	Indicates the status of the line card. States are: <ul style="list-style-type: none"> <li>• up—Line card is up.</li> <li>• sync—Line card is in synchronization with the main FIB.</li> <li>• FIB is repopulated on the line card.</li> <li>• reset—Line card FIB is reset.</li> <li>• reloading—Line card FIB is being reloaded.</li> <li>• disabled—Line card is disabled.</li> </ul>
CEF-XDR	Number of Cisco Express Forwarding XDR messages processed.
I/Fs	Interface numbers.

**Related Commands**

Command	Description
<b>show cef</b>	Displays which packets the line cards dropped or displays which packets were not express-forwarded.
<b>show cef interface</b>	Displays Cisco Express Forwarding-related interface information.
<b>show ipv6 cef</b>	Displays entries in the IPv6 FIB.

# show cef table

To display the configuration and operational state of the Cisco Express Forwarding Forwarding Information Base (FIB) table, use the **show cef table** command in privileged EXEC mode.

## Cisco IOS 12.2(33)SRB and Later S-Based Releases

```
show cef table [consistency-check | detail | internal | [ipv4 | ipv6] [vrf {* | Default | vrf-name}]
               [topology {* | base | topology-name}] [detail | internal]]
```

## Cisco IOS 12.4(20)T and Later T-Based Releases

```
show cef table [consistency-check | detail | internal | [ipv4 | ipv6] {Default | vrf-name} [detail |
               internal]]
```

### Syntax Description

<b>consistency-check</b>	(Optional) Displays the status of consistency checkers in the FIB.
<b>detail</b>	(Optional) Displays detailed Cisco Express Forwarding operational status and configuration.
<b>internal</b>	(Optional) Displays internal Cisco Express Forwarding operational status and configuration.
<b>ipv4</b>	(Optional) Displays operational status for IPv4 from the IPv4 FIB.
<b>ipv6</b>	(Optional) Displays operational status for IPv6 from the IPv6 FIB.
<b>vrf</b>	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance for the specified address family.
<b>*</b>	Displays operational status for all configured VRFs ( <b>vrf *</b> ) or all topologies ( <b>topology *</b> ), respectively.
<b>Default</b>	Displays operational status for the default VRF for the specified address family.
<i>vrf-name</i>	Displays operational status for the named VRF configured for the specified address family.
<b>topology</b>	(Optional) Specifies a topology for the selected address family.
<b>base</b>	Displays operational status for the base topology for the specified address family.
<i>topology-name</i>	Displays operational status for the identified topology-specific table.

### 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 2.2(28)SB.
12.2(33)SRA	This command was introduced.
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 this command to display information about the configuration and operational statistics for Cisco Express Forwarding IPv4 FIB and IPv6 FIB.

**Cisco IOS 12.4(20)T and Later T-based Releases**

When you enter an **ipv4** or **ipv6** keyword with the **show cef table** command, you must enter the name of a configured VRF or the **Default** keyword.

**Cisco IOS 12.2(33)SRB and Later S-based Releases**

The **vrf** and **topology** keywords are optional when you enter the **ipv4** or **ipv6** keyword with the **show cef table** command.

**Examples**

The following is sample output from the **show cef table** command:

```
Router# show cef table

Global information:
Output chain build favors:
  platform:      not configured
  CLI:          not configured
  operational:   convergence-speed
Output chain build characteristics:
  Inplace modify
    operational for:  load-sharing
  Collapse
    operational for:  load-sharing
  Indirection
    operational for:  recursive-prefix
MTRIE information:
  TAL: node pools:
    pool[C/8 bits]: 12 allocated (0 failed), 12480 bytes {1 refcount}

1 active IPv4 table (9 prefixes total) out of a maximum of 10000.
VRF          Prefixes      Memory  Flags
Default      9                13520

1 active IPv6 table (1 prefix total) out of a maximum of 10000.
VRF          Prefixes      Memory  Flags
VRF          Prefixes      Memory  Flags
Default      1                208
```

[Table 153](#) describes significant fields shown in the display.

**Table 153** *show cef table* Field Descriptions

Field	Description
Output chain build favors:	Indicates table output chain building operational preferences.
Platform: not configured	Output chain building characteristics are not explicitly set or supported by the platform. The default output chain building characteristics are used.
CLI: not configured	Output chain building characteristics are not explicitly configured. The default is used.
operational: convergence speed	Output chain building favors convergence. This is the default operational behavior.

**Table 153** show cef table Field Descriptions (continued)

Field	Description
Output chain build characteristics	Indicates the output chain building characteristics.
Inplace modify operational for: load-sharing	Indicates that the load sharing information in effect can be changed if the output information of the Interior Gateway Protocol (IGP) changes.
Collapse operational for: load-sharing	Indicates that the load-sharing tree is collapsed if load balancing is not affected.
Indirection operational for: recursive-prefix	Indicates that the use of indirection objects is enabled for recursive prefixes.
MTRIE information:	Indicates that information about the multi-array retrieval (MTRIE) follows.
TAL: node pools:	Indicates that node pool information for the Tree Abstraction Layer (TAL) follows.
pool (C/8 bits):	Indicates the memory management technique for the pool and the stride size (8 bits). The C indicates the use of a chunk pool. An M would indicate the use of a malloc.

The following is sample output from the **show cef table internal** command:

```
Router# show cef table internal

Table: IPv4:Default (id 0)
sources:          Default table
ref count:       31
flags (0x00):    none
smp allowed:     yes
default network: none
route count:     9
route count (fwd): 9
route count (non-fwd): 0
Database epoch:  0 (9 entries at this epoch)
Subblocks:

  These rates are ndbs/minute.
  RIB update rate:      0
  RIB update peak rate: 0
Internals:
table:                0x4BFA060
extra:                0x000000
broker record:       0x000000
tal root:            0x4C01988
lookup OCE:          0x4C12B50

Table: IPv6:Default (id 0)
sources:          Default table
ref count:       3
flags (0x00):    none
smp allowed:     no
default network: none
route count:     1
route count (fwd): 1
route count (non-fwd): 0
Database epoch:  0 (1 entry at this epoch)
```

```

Subblocks:

  These rates are ndbs/minute.
  RIB update rate:          0
  RIB update peak rate:    0
Internals:
  table:                    0x4BF9FF0
  extra:                    0x000000
  broker record:           0x000000
  tal root:                 0x4C96328
  lookup OCE:              0x4C12B30

```

Table 154 describes significant fields shown in the display.

**Table 154** *show cef table internal Field Descriptions*

Field	Description
Table: IPv4: Default (id 0)	The FIB table, IPv4 or IPv6, for which operation statistics follow.
sources: Default table	The source of the information comes from the Default table.
ref count: 3	The number of internal pointers to the VRF table structure.
flags (0x00): none	No flags are configured.
smp allowed: yes	Symmetrical Multi-Processing (SMP) is allowed.
default network: none	A default network is not configured.
route count: 9	Total number of routes is 9.
route count (fwd): 9	The number of routes forwarded is 9.
route count (non-fwd): 0	The number of routes not forwarded is 0.
Database epoch: 0 (9 entries at this epoch)	Epoch number (table version) is 0 and contains 9 entries.
Subblocks:	No subblocks are defined.
RIB update rate: 0	No update rate is configured for the RIB.
RIB update peak rate 0	No peak update rate is defined for the RIB.
Internal:	Identification for Cisco Express Forwarding internal operations.

The following is sample output from the **show cef table consistency-check** command:

```

Router# show cef table consistency-check

Consistency checker master control: enabled

IPv4:
Table consistency checker state:
  scan-rib-ios: disabled
    0/0/0/0 queries sent/ignored/checked/iterated
  scan-ios-rib: disabled
    0/0/0/0 queries sent/ignored/checked/iterated
  full-scan-rib-ios: enabled [1000 prefixes checked every 60s]
    0/0/0/0 queries sent/ignored/checked/iterated
  full-scan-ios-rib: enabled [1000 prefixes checked every 60s]
    0/0/0/0 queries sent/ignored/checked/iterated
Checksum data checking disabled

```

```
Inconsistency error messages are disabled
Inconsistency auto-repair is enabled (10s delay, 300s holddown)
Inconsistency auto-repair runs: 0
Inconsistency statistics: 0 confirmed, 0/16 recorded
```

## IPv6:

```
Table consistency checker state:
scan-ios-rib: disabled
  0/0/0/0 queries sent/ignored/checked/iterated
full-scan-rib-ios: enabled [1000 prefixes checked every 60s]
  0/0/0/0 queries sent/ignored/checked/iterated
full-scan-ios-rib: enabled [1000 prefixes checked every 60s]
  0/0/0/0 queries sent/ignored/checked/iterated
Checksum data checking disabled
Inconsistency error messages are disabled
Inconsistency auto-repair is enabled (10s delay, 300s holddown)
Inconsistency auto-repair runs: 0
Inconsistency statistics: 0 confirmed, 0/16 recorded
```

Table 155 describes significant fields shown in the display.

**Table 155** *show cef table consistency-check Field Descriptions*

Field	Description
scan-rib-ios: disabled	The consistency checker that compares the Routing Information Base (RIB) to the FIB table and provides the number of entries missing from the FIB table is disabled.
scan-ios-rib: disabled	The consistency checker that compares the FIB table to the RIB and provides the number of entries missing from the RIB is disabled.
full-scan-rib-ios: enabled	A full scan is enabled that compares the RIB to the FIB table. Every 60 seconds, 1000 prefixes are checked.
full-scan-ios-rib: enabled	A full scan is enabled that compares the FIB table to the RIB. Every 60 seconds, 1000 prefixes are checked.
Checksum data checking disabled	The data-checking function is disabled.
Inconsistency error messages are disabled	The consistency checker to generate inconsistency error messages is disabled.
Inconsistency auto-repair is enabled (10s delay, 300s holddown)	The auto repair function is enabled with the default settings of a 10-second delay and a 300-second holddown.

The following is sample output from the **show cef table IPv4 Default** command:

```
Router# show cef table ipv4 Default

Table: IPv4:Default (id 0)
sources:          Default table
ref count:       31
flags (0x00):    none
smp allowed:     yes
default network: none
route count:     9
route count (fwd): 9
route count (non-fwd): 0
Database epoch:  0 (9 entries at this epoch)
Subblocks:
```

```

These rates are ndbs/minute.
RIB update rate:          0
RIB update peak rate:    0

```

For a description of significant fields shown in the display, see [Table 154](#).

The following is sample output from the **show cef table IPv6 Default internal** command:

```

Router# show cef table ipv6 Default internal

Table: IPv6:Default (id 0)
sources:                Default table
ref count:              3
flags (0x00):          none
smp allowed:           no
default network:       none
route count:           1
route count (fwd):     1
route count (non-fwd): 0
Database epoch:        0 (1 entry at this epoch)
Subblocks:

These rates are ndbs/minute.
RIB update rate:       0
RIB update peak rate:  0
Internals:
table:                 0x4BF9FF0
extra:                 0x000000
broker record:        0x000000
tal root:              0x4C96328
lookup OCE:           0x4C12B30

```

For a description of significant fields shown in the display, see [Table 154](#).

#### Related Commands

Command	Description
<b>cef table consistency-check</b>	Enables Cisco Express Forwarding table consistency checker types and parameters.
<b>cef table output-chain build</b>	Configures Cisco Express Forwarding table output chain building characteristics for the forwarding of packet through the network.
<b>show cef</b>	Displays information about packets forwarded by Cisco Express Forwarding.

# show clns neighbors

To display end system (ES), intermediate system (IS), and multitopology Integrated Intermediate System-to-Intermediate System (M-ISIS) neighbors, use the **show clns neighbors** command in user EXEC or privileged EXEC mode.

**show clns neighbors** [*process-tag*] [*interface-type interface-number*] [**area**] [**detail**]

## Syntax Description

<i>process-tag</i>	(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 <b>null</b> 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.
<i>interface-type</i>	(Optional) Interface type.
<i>interface-number</i>	(Optional) Interface number.
<b>area</b>	(Optional) Displays the CLNS multiarea adjacencies.
<b>detail</b>	(Optional) Displays the area addresses advertised by the neighbor in the hello messages. Otherwise, a summary display is provided.  In IPv6, this keyword displays the address family of the adjacency.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The <b>area</b> and <b>detail</b> keywords were added.
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 <i>process-tag</i> 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 **show clns neighbors** command displays the adjacency that is learned through multitopology IS-IS for IPv6.

**Examples**

The following is sample output from the **show clns neighbors** command:

```
Router# show clns neighbors
```

System Id	Interface	SNPA	State	Holdtime	Type	Protocol
0000.0000.0007	Et3/3	aa00.0400.6408	UP	26	L1	IS-IS
0000.0C00.0C35	Et3/2	0000.0c00.0c36	Up	91	L1	IS-IS
0800.2B16.24EA	Et3/3	aa00.0400.2d05	Up	27	L1	M-ISIS
0800.2B14.060E	Et3/2	aa00.0400.9205	Up	8	L1	IS-IS

The following is sample output from the **show clns neighbors** command using the *process-tag* argument to display information about the VRF-aware IS-IS instance tag1:

```
Router# show clns tagRED neighbors
```

```
Tag tag1:
```

System Id	Interface	SNPA	State	Holdtime	Type	Protocol
igp-03	Fa0/	200d0.2b7f.9502	Up	9	L2	IS-IS
igp-03	PO2/2.1	DLCI 211	Up	27	L2	IS-IS
igp-02	PO2/0.1	DLCI 131	Up	29	L2	IS-IS
igp-11	Fa0/4	000e.d79d.7920	Up	7	L2	IS-IS
igp-11	Fa0/5	000e.d79d.7921	Up	8	L2	IS-IS
igp-11	PO3/2.1	DLCI 451	Up	24	L2	IS-IS

The following is sample output from the **show clns neighbors** command using the **detail** keyword:

```
Router# show clns neighbors detail
```

System Id	Interface	SNPA	State	Holdtime	Type	Protocol
0000.0000.0007	Et3/3	aa00.0400.6408	UP	26	L1	IS-IS

```
Area Address(es): 20
```

```
IP Address(es): 172.16.0.42*
```

```
Uptime: 00:21:49
```

0000.0C00.0C35	Et3/2	0000.0c00.0c36	Up	91	L1	IS-IS
----------------	-------	----------------	----	----	----	-------

```
Area Address(es): 20
```

```
IP Address(es): 192.168.0.42*
```

```
Uptime: 00:21:52
```

0800.2B16.24EA	Et3/3	aa00.0400.2d05	Up	27	L1	M-ISIS
----------------	-------	----------------	----	----	----	--------

```
Area Address(es): 20
```

```
IP Address(es): 192.168.0.42*
```

```
IPv6 Address(es): FE80::2B0:8EFF:FE31:EC57
```

```
Uptime: 00:00:27
```

```
Topology: IPv6
```

0800.2B14.060E	Et3/2	aa00.0400.9205	Up	8	L1	IS-IS
----------------	-------	----------------	----	---	----	-------

```
Area Address(es): 20
```

```
IP Address(es): 192.168.0.30*
```

```
Uptime: 00:21:52
```

The following is sample output from the **show clns neighbors** command using the *process-tag* argument to display information about the VRF-aware IS-IS instance tagSecond:

```
Router# show clns tagSecond neighbors
```

```
Tag tagSecond:
```

System Id	Interface	SNPA	State	Holdtime	Type	Protocol
igp-03	Fa0/2	00d0.2b7f.9502	Up	9	L2	IS-IS
igp-03	PO2/2.1	DLCI 211	Up	27	L2	IS-IS
igp-02	PO2/0.1	DLCI 131	Up	29	L2	IS-IS
igp-11	Fa0/4	000e.d79d.7920	Up	7	L2	IS-IS

```

igp-11          Fa0/5          000e.d79d.7921    Up    8          L2    IS-IS
igp-11          PO3/2.1       DLCI 451          Up    24         L2    IS-IS

```

Table 156 describes the significant fields shown in the display.

**Table 156** show clns neighbors Field Descriptions

Field	Description
Tag tagSecond	Tag name that identifies an IS-IS instance.
System Id	Six-byte value that identifies a system in an area.
Interface	Interface from which the system was learned.
SNPA	Subnetwork Point of Attachment. This is the data-link address.
State	State of the ES, IS, or M-ISIS.
Init	System is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent.
Up	Believes the ES or IS is reachable.
Holdtime	Number of seconds before this adjacency entry times out.
Type	The adjacency type. Possible values are as follows: <ul style="list-style-type: none"> <li>• ES—End-system adjacency either discovered via the ES-IS protocol or statically configured.</li> <li>• IS—Router adjacency either discovered via the ES-IS protocol or statically configured.</li> <li>• M-ISIS—Router adjacency discovered via the multitopology IS-IS protocol.</li> <li>• L1—Router adjacency for Level 1 routing only.</li> <li>• L1L2—Router adjacency for Level 1 and Level 2 routing.</li> <li>• L2—Router adjacency for Level 2 only.</li> </ul>
Protocol	Protocol through which the adjacency was learned. Valid protocol sources are ES-IS, IS-IS, ISO IGRP, Static, DECnet, and M-ISIS.

Notice that the information displayed in the **show clns neighbors detail** command output includes everything shown in **show clns neighbors** command output in addition to the area address associated with the IS neighbor and its uptime. When IP routing is enabled, Integrated-ISIS adds information to the output of the **show clns** commands. The **show clns neighbors detail** command output shows the IP addresses that are defined for the directly connected interface and an asterisk (\*) to indicate which IP address is the next hop.

# show clock

To display the time and date from the system software clock, use the **show clock** command in user EXEC or privileged EXEC mode.

**show clock [detail]**

Syntax Description	detail	(Optional) Indicates the clock source (NTP, VINES, hardware clock, and so on) and the current summer-time setting (if any).
--------------------	--------	---

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.

**Usage Guidelines** The software clock keeps an “authoritative” flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the “authoritative” flag is set, the flag prevents peers from synchronizing to the software clock.

The symbol that precedes the **show clock** display indicates the following:

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers	.15:29:03.158 UTC Tue Feb 25 2003:

These symbols are also used in NTP-based timestamping, such as for syslog (SEM) messages.



**Note**

In general, NTP synchronization takes approximately 15 to 20 minutes.

---

**Examples**

The following sample output shows that the current clock is authoritative and that the time source is NTP:

```
Router> show clock detail  
  
15:29:03.158 PST Tue Feb 25 2003  
Time source is NTP
```

The following example shows the current clock is authoritative, but NTP is not yet synchronized:

```
Router> show clock  
  
.16:42:35.597 UTC Tue Feb 25 2003
```

---

**Related Commands**

Command	Description
<b>clock set</b>	Manually sets the software clock.
<b>show calendar</b>	Displays the current time and date setting of the system hardware clock.

# show crypto engine

To display a summary of the configuration information for the crypto engines, use the **show crypto engine** command in privileged EXEC mode.

```
show crypto engine { accelerator { statistic | ring { control | packet | pool } } | brief | configuration
                   | connections { active | dh | dropped-packet | flow } | qos | token [detail]}
```

Syntax	Description
<b>accelerator</b>	Displays crypto accelerator information.
<b>statistic</b>	Displays crypto accelerator statistic information.
<b>ring</b>	Displays crypto accelerator ring information.
<b>control</b>	Displays control ring information.
<b>packet</b>	Displays packet ring information.
<b>pool</b>	Displays pool ring information.
<b>brief</b>	Displays a summary of the configuration information for the crypto engine.
<b>configuration</b>	Displays the version and configuration information for the crypto engine.
<b>connections</b>	Displays information about the crypto engine connections.
<b>active</b>	Displays all active crypto engine connections.
<b>dh</b>	Displays crypto engine Diffie-Hellman table entries.
<b>dropped-packet</b>	Displays crypto engine dropped packets.
<b>flow</b>	Displays crypto engine flow table entries.
<b>qos</b>	Displays quality of service (QoS) information. <ul style="list-style-type: none"> <li>This keyword has a null output if any advanced integration module (AIM) except AIM-VPN/SSL-1 is used. The command-line interface (CLI) will accept the command, but there will be no output.</li> </ul>
<b>token</b>	Displays the crypto token engine information.
<b>detail</b>	(Optional) Displays the detailed information of the crypto token engine.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	11.2	This command was introduced on the Cisco 7200, RSP7000, and 7500 series routers.
	12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
	12.4(4)T	IPv6 address information was added to command output.
	12.4(9)T	AIM-VPN/SSL-3 encryption module information was added to command output.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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(22)T	The <b>token</b> and <b>detail</b> keywords were added.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The <b>accelerator</b> , <b>control</b> , <b>packet</b> , <b>pool</b> , <b>ring</b> , and <b>static</b> keywords were added.

### Usage Guidelines

This command displays all crypto engines and displays the AIM-VPN product name.

If a hardware crypto engine does not support native Group Domain of Interpretation (GDOI) header preservation, the **show crypto engine connections active** output for Group Encrypted Transport VPN (GET VPN) IP security (IPsec) connections displays a disallowed IP address of 0.0.0.0 (see the **show crypto engine connections active** “Examples” section).

### Examples

The following is sample output from the **show crypto engine brief** command shows typical crypto engine summary information:

```
Router# show crypto engine brief

crypto engine name: Virtual Private Network (VPN) Module
                   crypto engine type: hardware
                               State: Enabled
                               Location: aim 0
VPN Module in slot: 0
  Product Name: AIM-VPN/SSL-3
  Software Serial #: 55AA
    Device ID: 001F - revision 0000
    Vendor ID: 0000
    Revision No: 0x001F0000
  VSK revision: 0
  Boot version: 255
  DPU version: 0
  HSP version: 3.3(18) (PRODUCTION)
  Time running: 23:39:30
    Compression: Yes
      DES: Yes
      3 DES: Yes
      AES CBC: Yes (128,192,256)
      AES CNTR: No
  Maximum buffer length: 4096
    Maximum DH index: 3500
    Maximum SA index: 3500
    Maximum Flow index: 7000
  Maximum RSA key size: 2048

crypto engine name: Cisco VPN Software Implementation
crypto engine type: software
  serial number: CAD4FCE1
crypto engine state: installed
crypto engine in slot: N/A
```

Table 157 describes the significant fields shown in the display.

**Table 157** show crypto engine brief Field Descriptions

Field	Description
crypto engine name	Name of the crypto engine as assigned with the <i>key-name</i> argument in the <b>crypto key generate dss</b> command.
crypto engine type	If “software” is listed, the crypto engine resides in either the Route Switch Processor (RSP) (the Cisco IOS crypto engine) or in a second-generation Versatile Interface Processor (VIP2).  If “crypto card” or “Encryption Service Adapter” (ESA) is listed, the crypto engine is associated with an ESA.
crypto engine state	The state “installed” indicates that a crypto engine is located in the given slot, but it is not configured for encryption.  The state “dss key generated” indicates the crypto engine found in that slot has Digital Signature Standard (DSS) keys already generated.
crypto engine in slot	Chassis slot number of the crypto engine. For the Cisco IOS crypto engine, this is the chassis slot number of the RSP.

The following is sample output from **show crypto engine** command shows IPv6 information:

```
Router# show crypto engine connections
```

```

  ID Interface  Type  Algorithm      Encrypt  Decrypt  IP-Address
  1 Et2/0       IPsec MD5           0        46 FE80::A8BB:CCFF:FE01:2C02
  2 Et2/0       IPsec MD5           41       0 FE80::A8BB:CCFF:FE01:2C02
  5 Tu0        IPsec SHA+DES      0         0
3FFE:2002::A8BB:CCFF:FE01:2C02
  6 Tu0        IPsec SHA+DES      0         0
3FFE:2002::A8BB:CCFF:FE01:2C02
 1001 Tu0        IKE    SHA+DES        0         0
3FFE:2002::A8BB:CCFF:FE01:2C02
```

The following **show crypto engine** command output displays information for a situation in which a hardware crypto engine does not support native GDOI:

```
Router# show crypto engine connections active
```

```
Crypto Engine Connections
```

```

ID Interface      Type  Algorithm      Encrypt  Decrypt  IP-Address
1079 Se0/0/0.10    IPsec AES+SHA      0         0 0.0.0.0
1080 Se0/0/0.10    IPsec AES+SHA      0         0 0.0.0.0
4364 <none>        IKE    SHA+3DES        0         0
4381 <none>        IKE    SHA+3DES        0         0
```

**Related Commands**

Command	Description
<b>crypto engine accelerator</b>	Enables the use of the onboard hardware accelerator for IPsec encryption.

# show crypto ikev2 policy

To display the default or a user-defined Internet Key Exchange Version 2 (IKEv2) policy, use the **show crypto ikev2 policy** command in privileged EXEC mode.

```
show crypto ikev2 policy [policy-name]
```

<b>Syntax Description</b>	<i>policy-name</i> (Optional) Displays the specified policy.
---------------------------	--

**Command Default** If no option is specified, then this command displays all the policies.

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	15.1(1)T	This command was introduced.
	15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
	Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

**Usage Guidelines** Use this command to display the default or user-defined IKEv2 policy. User-defined policies display the default values of the commands that are not explicitly configured under the policy.

**Examples** The following examples show the output for a default and user-defined policy.

## Default IKEv2 Policy

The default IKEv2 policy matches all local addresses in global VRF and uses the default IKEv2 proposal.

```
Router# show crypto ikev2 policy default
```

```
IKEv2 policy : default
  Match fvrf   : global
  Match address local : any
  Proposal     : default
```

```
Router# show crypto ikev2 policy default
```

This sample output shows the default IKEv2 policy that matches the local IPv6 address in global VRF:

```
IKEv2 policy : default
```

```
  Match fvrf   : global
  Match address local : 2001:DB8:1::1
  Proposal     : default
```

**User-defined IKEv2 policy**

```
Router# show crypto ikev2 policy policy-1
```

```

IKEv2 policy : policy-1
  Match fvrf : green
  Match local : 10.0.0.1
  Proposal   : proposal-A
  Proposal   : proposal-B

```

Table 158 describes the significant fields shown in the display.

**Table 158** *show crypto ikev2 policy Field Descriptions*

Field	Description
IKEv2 policy	Name of the IKEv2 policy.
Match fvrf	The front door virtual routing and forwarding (FVRF) specified for matching the IKEv2 policy.
Match local	The local IP address (IPv4 or IPv6) assigned for matching the IKEv2 policy.
Proposal	The name of the proposal that is attached to the IKEv2 policy.

**Related Commands**

Command	Description
<b>crypto ikev2 policy</b>	Defines an IKEv2 policy.
<b>crypto ikev2 proposal</b>	Defines an IKE proposal.
<b>match (ikev2 policy)</b>	Matches an IKEv2 policy based on the parameters.
<b>proposal</b>	Specifies the proposals that must be used in the IKEv2 policy.

# show crypto ikev2 profile

To display a user-defined Internet Key Exchange Version 2 (IKEv2) profile, use the **show crypto ikev2 profile** command in privileged EXEC mode.

```
show crypto ikev2 profile [profile-name]
```

<b>Syntax Description</b>	<i>profile-name</i> (Optional) Name of the IKEv2 profile.
---------------------------	---

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	15.1(1)T	This command was introduced.
	15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
	Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

<b>Usage Guidelines</b>	Use this command to display information about an IKEv2 profile. This command also displays the default values of the commands that are not explicitly configured in the IKEv2 profile. If a profile name is not specified, the command displays all the user-defined IKEv2 profiles.
-------------------------	--

<b>Examples</b>	The following example is sample output from the <b>show crypto ikev2 profile</b> command:
-----------------	---

```
Router# show crypto ikev2 profile

IKEv2 profile: prof
Ref Count: 3
Match criteria:
  Fvrf: any
  Local address/interface: none
Identities:
  fqdn smap-initiator
Certificate maps: none
Local identity: fqdn dmap-responder
Remote identity: none
Local authentication method: pre-share
Remote authentication method(s): pre-share
Keyring: v2-kr1
Trustpoint(s): none
Lifetime: 86400 seconds
DPD: disabled
NAT-keepalive: disabled
Ivrf: global
```

```
Virtual-template: none
Accounting mlist: none
```

Table 158 describes the significant fields shown in the display.

**Table 159** *show crypto ikev2 profile Field Descriptions*

Field	Description
IKEv2 profile	Name of the IKEv2 profile.
Match	The match parameter in the profile.
Local Identity	The local identity type.
Local authentication method	The local authentication methods.
Remote authentication method	The remote authentication methods.
Keyring	The keyring specified in the profile.
Trustpoint	The trustpoints used in the Rivest, Shamir and Adleman (RSA) signature authentication method.
Lifetime	The lifetime of the IKEv2 profile.
DPD	The status of Dead Peer Detection (DPD).
Ivrf	The Inside VRF (IVRF) in the profile.
Virtual-template	The virtual template in the profile.

# show crypto ikev2 sa

To display the Internet Key Exchange Version 2 (IKEv2) security associations (SA), use the **show crypto ikev2 sa** command in privileged EXEC mode.

```
show crypto ikev2 sa {local [ipv4-address | ipv6-address] | remote [ipv4-address | ipv6-address] |
  fvrfrf vrf-name} [detailed]
```

## Syntax Description

<b>local</b> [ipv4-address   ipv6-address]	Displays the current IKEv2 security associations matching the local IP address.
<b>remote</b> [ipv4-address   ipv6-address]	Displays the current IKEv2 security associations matching the remote IP address.
<b>fvrfrf</b> vrf-name	Displays the current IKEv2 security associations matching the specified front door virtual routing and forwarding (FVRF).
<b>detailed</b>	(Optional) Displays detailed information about the current security associations.

## Command Default

All the current IKEv2 security associations are displayed.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

## Usage Guidelines

Use this command to display information about the current IKEv2 security associations.

## Examples

The following are sample outputs from the **show crypto ikev2 sa** command:

```
Router# show crypto ikev2 sa
```

```
Tunnel-id  Local          Remote          fvrfrf/ivrf      Status
2          10.0.0.1/500    10.0.0.2/500  (none)/(none)    READY
           Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
           Life/Active Time: 86400/361 sec
```

```
Router# show crypto ikev2 sa
```

```
Tunnel-id  Local          Remote          fvrfrf/ivrf      Status
1          2001:DB8:0::1/500  2001:DB8:0::2/500  (none)/(none)    READY
           Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
```

Life/Active Time: 86400/361 sec

The following is sample output from the **show crypto ikev2 sa detailed** command:

Router# **show crypto ikev2 sa detailed**

```
Tunnel-id   Local           Remote           fvrf/ivrf       Status
2           10.0.0.1/500   10.0.0.2/500   (none)/(none)   READY
  Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
  Life/Active Time: 86400/479 sec
  CE id: 0, Session-id: 2, MIB-id: 2
  Status Description: Negotiation done
  Local spi: BCF1453548BE731C      Remote spi: 85CB158F05817B3A
  Local id: 10.0.0.1      Remote id: 10.0.0.2
  Local req mess id: 3      Remote req mess id: 0
  Local next mess id: 3      Remote next mess id: 1
  Local req queued: 3      Remote req queued: 0
  Local window: 5      Remote window: 5
  DPD configured for 0 seconds
  NAT-T is not detected
```

Table 160 describes the significant fields shown in the display.

**Table 160** *show crypto ikev2 sa detailed* Field Descriptions

Field	Description
Tunnel-id	Unique identifier of the IKEv2 tunnel.
Local	IP address (IPv4 or IPv6) and UDP port of the local IKEv2 endpoint.
Remote	IP address (IPv4 or IPv6) and UDP port of the remote IKEv2 endpoint.
fvrf/ivrf	FVRF/IVRF of the local IKEv2 endpoint.
Status	Status of the IKEv2 tunnel.
Encr	Encryption algorithm used by the IKEv2 tunnel.
Hash	Integrity algorithm used by the IKEv2 tunnel.
DH Grp	Diffie-Hellman (DH) group used by the IKEv2 tunnel.
Auth Sign	Authentication method used by the local IKEv2 endpoint.
Auth Verify	Authentication method used by the remote IKEv2 endpoint.
Life/Active Time	The total and active lifetime of the IKEv2 tunnel.
CE id	The crypto engine ID used by the local IKEv2 endpoint.
Session-id	The session ID for the IKEv2 tunnel.
MIB-id	The MIB identifier for the IKEv2 tunnel.
Status Description	Description of the IKEv2 tunnel status.
Local spi	IKEv2 security parameter index (SPI) of the local IKEv2 endpoint.
Remote spi	IKEv2 SPI of the remote IKEv2 endpoint.
Local id	IKEv2 identity of the local IKEv2 endpoint
Remote id	IKEv2 identity of the remote IKEv2 endpoint.
Local req mess id	Message ID of the last IKEv2 request sent.

**Table 160** *show crypto ikev2 sa detailed Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Remote req mess id	Message ID of the last IKEv2 request received.
Local next mess id	Message ID of the next IKEv2 request to be sent.
Remote next mess id	Message ID of the next IKEv2 request to be received.
Local req queued	Number of requests queued to be sent.
Remote req queued	Number of requests queued to be processed.
Local window	IKEv2 window size of the local IKEv2 endpoint.
Remote window	IKEv2 window size of the remote IKEv2 endpoint.
DPD	DPD interval.
NAT_T	NAT detection status.

# show crypto ikev2 session

To display the status of active Internet Key Exchange Version 2 (IKEv2) sessions, use the **show crypto ikev2 session** command in privileged EXEC mode.

**show crypto ikev2 session [detailed]**

Syntax Description	detailed	(Optional) Displays detailed information about the session.
--------------------	----------	---

**Command Default** The session information is displayed in a brief format.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	15.1(1)T	This command was introduced.
	15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
	Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

**Usage Guidelines** Use this command to display information about the active IKEv2 sessions. Use the **detailed** keyword to display information about IKEv2 parent and child security associations.

**Examples** The following is a sample output from the **show crypto ikev2 session** and **show crypto ikev2 session detailed** command.

```
Router# show crypto ikev2 session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id  Local          Remote          fvrf/ivrf      Status
1          10.0.0.1/500    10.0.0.2/500    (none)/(none)  READY
           Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
           Life/Active Time: 86400/65 sec
Child sa: local selector 10.0.0.1/0 - 10.0.0.1/65535
           remote selector 10.0.0.2/0 - 10.0.0.2/65535
           ESP spi in/out: 0x9360A95/0x6C340600
           CPI in/out: 0x9FE5/0xC776

Router# show crypto ikev2 session detailed

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id  Local          Remote          fvrf/ivrf      Status
1          10.0.0.1/500    10.0.0.2/500    (none)/(none)  READY
           Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
```

```

Life/Remaining/Active Time: 86400/86157/248 sec
CE id: 0, Session-id: 1, MIB-id: 1
Status Description: Negotiation done
Local spi: 750CBE827434A245      Remote spi: 4353FEDBABEBF24C
Local id:      10.0.0.1          Remote id:      10.0.0.2
Local req mess id: 0            Remote req mess id: 0
Local next mess id: 0          Remote next mess id: 2
Local req queued: 0            Remote req queued: 0
Local window: 5                Remote window: 5
DPD configured for 0 seconds
NAT-T is not detected
Child sa: local selector 10.0.0.1/0 - 10.0.0.1/65535
         remote selector 10.0.0.2/0 - 10.0.0.2/65535
         ESP spi in/out: 0x9360A95/0x6C340600
         CPI in/out: 0x9FE5/0xC776
         AH spi in/out: 0x0/0x0
         Encr: AES CBC, keysize: 128, esp_hmac: SHA96
         ah_hmac: Unknown - 0, comp: IPCOMP_LZS, mode tunnel

```

Table 160 describes the significant fields shown in the display.

**Table 161** *show crypto ikev2 session detailed Field Descriptions*

Field	Description
Tunnel id	Unique identifier of IKEv2 tunnel.
Local	IP address (IPv4 or IPv6) and UDP port of the local IKEv2 endpoint.
Remote	IPv4 or IPv6 address and UDP port of the remote IKEv2 endpoint.
fvr/ivrf	FVRF/IVRF of the local IKEv2 endpoint.
Status	Status of the IKEv2 tunnel.
Encr	Encryption algorithm used by the IKEv2 tunnel.
Hash	Integrity algorithm used by the IKEv2 tunnel.
DH Grp	DH group used by the IKEv2 tunnel.
Auth Sign	Authentication method used by the local IKEv2 endpoint.
Auth Verify	Authentication method used by the remote IKEv2 endpoint.
Life/Active Time	The total and active lifetime of the IKEv2 tunnel.
CE id	The crypto engine ID used by the local IKEv2 endpoint.
Session-id	The session ID for the IKEv2 tunnel.
MIB-id	The MIB identifier for the IKEv2 tunnel.
Status Description	Description of the IKEv2 tunnel status.
Local spi	IKEv2 security parameter index (SPI) of the local IKEv2 endpoint.
Remote spi	IKEv2 SPI of the remote IKEv2 endpoint.
Local id	IKEv2 identity of the local IKEv2 endpoint
Remote id	IKEv2 identity of the remote IKEv2 endpoint.
Local req mess id	Message ID of the last IKEv2 request sent.
Remote req mess id	Message ID of the last IKEv2 request received.

**Table 161** *show crypto ikev2 session detailed Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Local next mess id	Message ID of the next IKEv2 request to be sent.
Remote next mess id	Message ID of the next IKEv2 request to be received.
Local req queued	Number of requests queued to be sent.
Remote req queued	Number of requests queued to be processed.
Local window	IKEv2 window size of the local IKEv2 endpoint.
Remote window	IKEv2 window size of the remote IKEv2 endpoint.
DPD	DPD interval.
NAT	NAT detection status.
Child sa: local selector	Local network protected by the child security association (SA).
remote selector	Remote network protected by the child SA.
ESP spi in/out	Inbound and outbound SPI of the Encapsulating Security Payload (ESP) child SA.
CPI in/out	Inbound and outbound Cisco Product Identification (CPI) of the IP compression (IPComp) child SA.
AH spi in/out	Inbound and outbound SPI of the Authentication Header (AH) child SA.
Encr	Encryption algorithm used by the ESP child SA.
keysize	Size of the key in bits used by the encryption algorithm.
esp_hmac	Integrity algorithm used by the ESP child SA.
ah_hmac	Integrity algorithm used in the AH child SA, if available.
comp	Compression algorithm used by IPComp child SA.
mode	Tunnel or transport mode used by ESP/AH child SA.

# show crypto ipsec policy

To display the parameters for each IP Security (IPsec) policy, use the **show crypto ipsec policy** command in user EXEC or privileged EXEC mode.

```
show crypto ipsec policy [name policy-name]
```

<b>Syntax Description</b>	<b>name <i>policy-name</i></b> (Optional) The specific policy for which parameters will be displayed.
---------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(4)T	This command was introduced.
	12.4(4)T	Support for IPv6 was added.
	Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

<b>Usage Guidelines</b>	If no policy is specified, then information about all policies is displayed.
-------------------------	--

<b>Examples</b>	The following is sample output from the <b>show crypto ipsec policy</b> command:
-----------------	--

```
Router# show crypto ipsec policy

Crypto IPsec client security policy data

Policy name:      OSPFv3-1-1000
Policy refcount:  1
Inbound AH SPI:  1000 (0x3E8)
Outbound AH SPI: 1000 (0x3E8)
Inbound AH Key:   1234567890ABCDEF1234567890ABCDEF
Outbound AH Key:  1234567890ABCDEF1234567890ABCDEF
Transform set:    ah-md5-hmac
```

[Table 162](#) describes the significant fields shown in the display.

**Table 162** *show crypto ipsec policy* Field Descriptions

Field	Description
Policy name	Specifies the name of the policy.
Inbound AH SPI	The authentication header (AH) security policy index (SPI) for inbound links.
Outbound AH SPI	The AH SPI for outbound links.
Inbound AH Key	The AH key for inbound links.

**Table 162** *show crypto ipsec policy Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Outbound AH Key	The AH key for outbound links.
Transform set	The transform set, which is an acceptable combination of security protocols and algorithms.

# show crypto ipsec sa

To display the settings used by current security associations (SAs), use the **show crypto ipsec sa** command in privileged EXEC mode.

```
show crypto ipsec sa [map map-name | address | identity | interface type number | peer
[vrf fvr-name] address | vrf ivrf-name | ipv6 [interface type number]] [detail]
```

## IPsec and IKE Stateful Failover Syntax

```
show crypto ipsec sa [active | standby]
```

Syntax Description		
<b>map</b> <i>map-name</i>	(Optional) Displays any existing SAs that were created for the crypto map set with the value for the <i>map-name</i> argument.	
<b>address</b>	(Optional) Displays all existing SAs, sorted by the destination address (either the local address or the address of the IP security (IPsec) remote peer) and then by protocol (Authentication Header [AH] or Encapsulation Security Protocol [ESP]).	
<b>identity</b>	(Optional) Displays only the flow information. SA information is not shown.	
<b>interface</b> <i>type number</i>	(Optional) Displays all existing SAs created for the interface value provided in the <i>interface</i> argument.	
<b>peer</b> [ <b>vrf</b> <i>fvr-name</i> ] <b>address</b>	(Optional) Displays all existing SAs with the peer address. If the peer address is in the Virtual Routing and Forwarding (VRF), specify <b>vrf</b> and the <i>fvr-name</i> .	
<b>vrf</b> <i>ivrf-name</i>	(Optional) Displays all existing SAs whose inside virtual routing and forwarding (IVRF) is the same as the valued used for the <i>ivrf-name</i> argument.	
<b>ipv6</b>	(Optional) Displays IPv6 crypto IPsec SAs.	
<b>detail</b>	(Optional) Detailed error counters. (The default is the high-level send or receive error counters.)	
<b>active</b>	(Optional) Displays high availability (HA) - enabled IPsec SAs that are in the active state.	
<b>standby</b>	(Optional) Displays HA-enabled IPsec SAs that are in the standby state.	

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	11.3T	This command was introduced.
	12.2(13)T	The “remote crypto endpt” and “in use settings” fields were modified to support Network Address Translation (NAT) traversal.

Release	Modification
12.2(15)T	The <b>interface</b> keyword and <i>type</i> and <i>number</i> arguments were added. The <b>peer</b> keyword, the <b>vrf</b> keyword, and the <i>fvr-f-name</i> argument were added. The <b>address</b> keyword was added to the <b>peer</b> keyword string. The <b>vrf</b> keyword and <i>ivrf-name</i> argument were added.
12.3(11)T	The <b>active</b> and <b>standby</b> keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
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.
Cisco IOS XE Release 2.1	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

If no keyword is used, all SAs are displayed. They are sorted first by interface and then by traffic flow (for example, source or destination address, mask, protocol, or port). Within a flow, the SAs are listed by protocol (ESP or AH) and direction (inbound or outbound).

### Examples

The following is sample output from the **show crypto ipsec sa** command:

```
Router# show crypto ipsec sa

interface: Tunnel1
  Crypto map tag: Tunnel1-head-0, local addr 10.5.5.2
  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.5.5.2/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (10.5.5.1/255.255.255.255/47/0)
  current_peer 10.5.5.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 492908510, #pkts encrypt: 492908510, #pkts digest: 492908510
    #pkts decaps: 492908408, #pkts decrypt: 492908408, #pkts verify: 492908408
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 55, #recv errors 0

  local crypto endpt.: 10.5.5.2, remote crypto endpt.: 10.5.5.1
  path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2
  current outbound spi: 0xDE4EE29D(3729711773)

  inbound esp sas:
    spi: 0xC06CA92B(3228346667)
      transform: esp-3des esp-sha-hmac ,
      in use settings = {Tunnel, }
      conn id: 3139, flow_id: VSA:1139, crypto map: Tunnel1-head-0
      sa timing: remaining key lifetime (k/sec): (3948785/556)
      IV size: 8 bytes
      replay detection support: Y
      Status: ACTIVE

  inbound ah sas:
    spi: 0xC87AB936(3363486006)
      transform: ah-md5-hmac ,
      in use settings = {Tunnel, }
```

```

conn id: 3139, flow_id: VSA:1139, crypto map: Tunnell-head-0
sa timing: remaining key lifetime (k/sec): (3948785/556)
replay detection support: Y
Status: ACTIVE

inbound pcp sas:

outbound esp sas:
spi: 0xDE4EE29D(3729711773)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 3140, flow_id: VSA:1140, crypto map: Tunnell-head-0
sa timing: remaining key lifetime (k/sec): (3948785/556)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
spi: 0xAEEDD4F1(2934822129)
transform: ah-md5-hmac ,
in use settings ={Tunnel, }
conn id: 3140, flow_id: VSA:1140, crypto map: Tunnell-head-0
sa timing: remaining key lifetime (k/sec): (3948785/556)
replay detection support: Y
Status: ACTIVE

outbound pcp sas:

```

The following is sample output from the **show crypto ipsec sa identity detail** command:

```
Router# show crypto ipsec sa identity detail
```

```

interface: Tunnell
  Crypto map tag: Tunnell-head-0, local addr 10.5.5.2
  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer (none) port 500
  DENY, flags={ident_is_root,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
  #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
  #pkts invalid prot (rcv) 0, #pkts verify failed: 0
  #pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
  ##pkts replay failed (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv) 0

  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.5.5.2/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (10.5.5.1/255.255.255.255/47/0)
  current_peer 10.5.5.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 492923510, #pkts encrypt: 492923510, #pkts digest: 492923510
  #pkts decaps: 492923408, #pkts decrypt: 492923408, #pkts verify: 492923408
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #pkts no sa (send) 55, #pkts invalid sa (rcv) 0
  #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0

```

```
#pkts invalid prot (rcv) 0, #pkts verify failed: 0
#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv) 0
```

Table 163 describes the significant fields shown in the above displays (**show crypto ipsec sa** and **show crypto ipsec sa detail**).

**Table 163** *show crypto ipsec sa Field Descriptions*

Field	Description
crypto map tag	Policy tag for IPsec.
protected vrf	IVRF name that applies to the IPsec interface.
local ident (addr/mask/prot/port)	Local selector that is used for encryption and decryption.
remote ident (addr/mask/prot/port)	Remote selector that is used for encryption and decryption.
current peer	Current peer with which the IPsec tunnel communicates.
PERMIT, flags	IPsec SA is triggered by the Access Control List (ACL) permit action.
pkts encaps	Statistics number of packets that were successfully encapsulated by IPsec.
pkts encrypt	Statistics number of packets that were successfully encrypted by IPsec.
pkts digest	Statistics number of packets that were successfully hash digested by IPsec.
pkts decaps	Statistics number of packets that were successfully decapsulated by IPsec.
pkts decrypt	Statistics number of packets that were successfully decrypted by IPsec.
pkts verify	Received packets that passed the hash digest check.
pkts compressed	Number of packets that were successfully compressed by IPsec.
pkts decompressed	Number of packets that were successfully decompressed by IPsec.
pkts not compressed	Number of outbound packets that were not compressed.
pkts compr. failed	Number of packets that failed compression by IPsec.
pkts not decompressed	Number of inbound packets that were not compressed.
pkts decompress failed	Number of packets that failed decompression by IPsec.
send errors	Number of outbound packets that had errors.
rcv errors	Number of inbound packets that had errors.
local crypto endpt.	Local endpoint terminated by IPsec.
remote crypto endpt.	Remote endpoint terminated by IPsec.

**Table 163** *show crypto ipsec sa Field Descriptions*

<b>Field</b>	<b>Description</b>
path mtu	Maximum transmission unit (MTU) size that is figured based on the Internet Control Message Protocol (ICMP) unreachable packet. This value also has to consider the IPsec overhead.
ip mtu	Interface MTU size that considers the IPsec overhead.
current outbound spi	Current outbound Security Parameters Index (SPI).
ip mtu idb	Interface description block (IDB) that is used to determine the crypto IP MTU.
current outbound spi	Current outbound Security Parameter Index (SPI).
inbound esp sas	Encapsulating Security Payload (ESP) for the SA for the inbound traffic.
spi	SPI for classifying the inbound packet.
transform	Security algorithm that is used to provide authentication, integrity, and confidentiality.
in use settings	Transform that the SA uses (for example: tunnel mode, transport mode, UDP-encapsulated tunnel mode, or UDP-encapsulated transport mode).
conn id	ID that is stored in the crypto engine to identify the IPsec/Internet Key Exchange (IKE) SA.
flow_id	SA identity.
crypto map	Policy for the IPsec.
sa timing: remaining key lifetime (k/sec)	Seconds or kilobytes remaining before a rekey occurs.
IV size	Size of the initialization vector that is used for the cryptographic synchronization data used to encrypt the payload.
replay detection support	A specific SA has enabled the replay detection feature.
inbound ah sas	Authentication algorithm for the SA for inbound traffic.
inbound pcg sas	Compression algorithm for the SA for inbound traffic.
outbound esp sas	Encapsulating security payload for the SA for outbound traffic.
outbound ah sas	Authentication algorithm for the SA for outbound traffic.
outbound pcg sas	Compression algorithm for the SA for outbound traffic.
DENY, flags	IPsec SA is triggered by the ACL deny action.
pkts decompress failed	Number of packets decompressed by IPsec that failed.
pkts no sa (send)	Outbound packets cannot find the associated IPsec SA.
pkts invalid sa (rcv)	Received packets that failed the IPsec format check.
pkts invalid prot (recv)	Received packets that have the wrong protocol field.
pkts verify failed	Received packets that failed the hash digest check.

**Table 163** *show crypto ipsec sa Field Descriptions*

Field	Description
pkts invalid identity (rcv)	Packets after decryption cannot find the associated selector.
pkts pkts invalid len (rcv)	For the software crypto engine, inbound packets that have an incorrect pad length.
pkts replay rollover (send)	Sent packets that failed the replay test check.
pkts replay rollover (rcv)	Received packets that failed the replay test check.
pkts internal err (send)	Sent packets that failed because of a software or hardware error.
pkts internal err (rcv)	Received packets that failed because of a software or hardware error.
protected vrf	IVRF name that applies to the IPsec interface.

**show crypto ipsec sa vrf Command Output**

The following is sample output from the **show crypto ipsec sa vrf** command:

```
Router# show crypto ipsec sa vrf vpn2

interface: Ethernet1/2
  Crypto map tag: ra, local addr. 172.16.1.1

  protected vrf: vpn2
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.4.1.4/255.255.255.255/0/0)
  current_peer: 10.1.1.1:500
    PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

  local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.1.1.1
  path mtu 1500, media mtu 1500
  current outbound spi: 50110CF8

  inbound esp sas:
    spi: 0xA3E24AFD(2749516541)
      transform: esp-3des esp-md5-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 5127, flow_id: 7, crypto map: ra
      sa timing: remaining key lifetime (k/sec): (4603517/3503)
      IV size: 8 bytes
      replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
    spi: 0x50110CF8(1343294712)
      transform: esp-3des esp-md5-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 5128, flow_id: 8, crypto map: ra
```

```

sa timing: remaining key lifetime (k/sec): (4603517/3502)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

```

The following configuration was in effect when the preceding **show crypto ipsec sa vrf** command was issued. The IPsec remote access tunnel was “UP” when this command was issued.

```

crypto dynamic-map vpn1 1
 set transform-set vpn1
 set isakmp-profile vpn1-ra
 reverse-route
!
crypto dynamic-map vpn2 1
 set transform-set vpn2
 set isakmp-profile vpn2-ra
 reverse-route
!
!
crypto map ra 1 ipsec-isakmp dynamic vpn1
crypto map ra 2 ipsec-isakmp dynamic vpn2

```

[Table 164](#) describes the significant fields shown in the preceding **show crypto ipsec sa vrf** display. Additional fields are self-explanatory or can be found in [Table 164](#).

**Table 164** *show crypto ipsec sa vrf Field Descriptions*

Field	Description
remote crypto endpt.	Remote endpoint terminated by IPsec.
media mtu	MTU value for media, such as an Ethernet or a serial interface.
inbound esp sas	Encapsulating security payload for the SA of the inbound traffic.

### IPsec and IKE Stateful Failover Examples

The following sample output shows the IPsec SA status of only the active device:

```

Router# show crypto ipsec sa active

interface: Ethernet0/0
  Crypto map tag: to-peer-outside, local addr 10.165.201.3

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
current_peer 209.165.200.225 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
  path mtu 1500, media mtu 1500

```

```

current outbound spi: 0xD42904F0(3559458032)

inbound esp sas:
spi: 0xD3E9ABD0(3555306448)
  transform: esp-3des ,
  in use settings ={Tunnel, }
  conn id: 2006, flow_id: 6, crypto map: to-peer-outside
  sa timing: remaining key lifetime (k/sec): (4586265/3542)
    HA last key lifetime sent(k): (4586267)
  ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

```

[Table 165](#) describes the significant fields shown in the preceding **show crypto ipsec sa active** display. Additional fields are self-explanatory or can be found in [Table 165](#) or [Table 164](#).

**Table 165** *show crypto ipsec sa active Field Descriptions.*

Field	Description
HA last key lifetime sent (k)	Last stored kilobytes lifetime value for HA.
ike_cookies	ID that identifies the IKE SAs.

The following sample output shows the IPsec SA status of only the standby device. The fields in the display are either self-explanatory or can be found in [Table 163](#), [Table 164](#), or [Table 165](#).

Router# **show crypto ipsec sa standby**

```

interface: Ethernet0/0
  Crypto map tag: to-peer-outside, local addr 10.165.201.3

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
current_peer 209.165.200.225 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
  path mtu 1500, media mtu 1500
  current outbound spi: 0xD42904F0(3559458032)

inbound esp sas:
spi: 0xD3E9ABD0(3555306448)
  transform: esp-3des ,
  in use settings ={Tunnel, }
  conn id: 2012, flow_id: 12, crypto map: to-peer-outside
  sa timing: remaining key lifetime (k/sec): (4441561/3486)
    HA last key lifetime sent(k): (4441561)
  ike_cookies: 00000000 00000000 00000000 00000000
  IV size: 8 bytes
  replay detection support: Y
  Status: STANDBY

inbound ah sas:

```

■ **show crypto ipsec sa**

```

spi: 0xF3EE3620(4092474912)
  transform: ah-md5-hmac ,
  in use settings =(Tunnel, )
  conn id: 2012, flow_id: 12, crypto map: to-peer-outside
  sa timing: remaining key lifetime (k/sec): (4441561/3486)
    HA last key lifetime sent(k): (4441561)
  ike_cookies: 00000000 00000000 00000000 00000000
  replay detection support: Y
  Status: STANDBY

inbound pcp sas:

outbound esp sas:
spi: 0xD42904F0(3559458032)
  transform: esp-3des ,
  in use settings =(Tunnel, )
  conn id: 2011, flow_id: 11, crypto map: to-peer-outside
  sa timing: remaining key lifetime (k/sec): (4441561/3485)
    HA last key lifetime sent(k): (4441561)
  ike_cookies: 00000000 00000000 00000000 00000000
  IV size: 8 bytes
  replay detection support: Y
  Status: STANDBY

outbound ah sas:
spi: 0x75251086(1965363334)
  transform: ah-md5-hmac ,
  in use settings =(Tunnel, )
  conn id: 2011, flow_id: 11, crypto map: to-peer-outside
  sa timing: remaining key lifetime (k/sec): (4441561/3485)
    HA last key lifetime sent(k): (4441561)
  ike_cookies: 00000000 00000000 00000000 00000000
  replay detection support: Y
  Status: STANDBY

outbound pcp sas:

```

---

**Related Commands**

Command	Description
<b>crypto ipsec security-association</b>	Configures the IPSec security associations.

---

# show crypto isakmp key

To list the keyrings and their preshared keys, use the **show crypto isakmp key** command in privileged EXEC mode.

## show crypto isakmp key

### 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(4)T	IPv6 address information was added to command output.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

### Examples

The following is sample output for the **show crypto isakmp key** command:

```
Router# show crypto isakmp key

Hostname/Address      Preshared Key
vpn1                  : 172.61.1.1      vpn1
vpn2                  : 10.1.1.1        vpn2
```

The following configuration was in effect when the above **show crypto isakmp key** command was issued:

```
crypto keyring vpn1
  pre-shared-key address 172.16.1.1 key vpn1
crypto keyring vpn2
  pre-shared-key address 10.1.1.1 key vpn2
```

[Table 166](#) describes significant fields in the **show crypto isakmp key** profile.

**Table 166** *show crypto isakmp key Field Descriptions*

Field	Description
Hostname/Address	The preshared key host name or address.
Preshared Key	The preshared key.
keyring	Name of the crypto keyring. The global keys are listed in the default keyring.
VRF string	The Virtual Private Network routing and forwarding (VRF) of the keyring. If the keyring does not have a VRF, an empty string is printed.

# show crypto isakmp peers

To display the Internet Security Association and Key Management Protocol (ISAKMP) peer descriptions, use the **show crypto isakmp peers** command in privileged EXEC mode.

```
show crypto isakmp peers [ipaddress | ipv6address | config [peername]]
```

## Syntax Description

*ipaddress* (Optional) The IP address of the specific peer.



**Note** If the optional *ipaddress* argument is not included with the command, a summarization of all peers is displayed.

*ipv6address* (Optional) The IPv6 address of the specific peer.

**config** (Optional) Displays detailed information about all peers or a specific peer.

*peername* (Optional) The peer name.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The <b>config</b> keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	The <b>show crypto isakmp peer</b> command name was changed to <b>show crypto isakmp peers</b> .
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 on the Cisco ASR 1000 Series Routers.

## Usage Guidelines

Before you can use the **config** keyword, the following commands must be enabled for the accounting update to work correctly: **aaa accounting update** with **new info** keyword and **radius-server vsa send** with **accounting** keyword.

## Examples

The following output example shows information about the peer named “This-is-another-peer-at-10-1-1-3”:

```
Router# show crypto isakmp peers
```

```
Peer: 10.1.1.3 Port: 500
Description: This-is-another-peer-at-10-1-1-3
Phase1 id: 10.1.1.3
```

In the following example, the **config** keyword is used to display all manageability information for an Easy VPN remote device. Cisco Easy VPN is an IP Security (IPsec) virtual private network (VPN) solution supported by Cisco routers and security appliances. It greatly simplifies VPN deployment for remote offices and mobile workers. The fields are self-explanatory.

```
Router# show crypto isakmp peers config
```

```
Client-Public-Addr=192.168.10.2:500; Client-Assigned-Addr=172.16.1.209;
Client-Group=branch; Client-User=branch; Client-Hostname=branch.; Client-Platform=Cisco
1711; Client-Serial=FOC080210E2 (412454448); Client-Config-Version=11;
Client-Flash=33292284; Client-Available-Flash=10202680; Client-Memory=95969280;
Client-Free-Memory=14992140; Client-Image=flash:c1700-advipservicesk9-mz.ef90241;
```

```
Client-Public-Addr=192.168.10.3:500; Client-Assigned-Addr=172.16.1.121;
Client-Group=store; Client-User=store; Client-Hostname=831-storerouter.;
Client-Platform=Cisco C831; Client-Serial=FOC08472UXR (1908379618);
Client-Config-Version=2; Client-Flash=24903676; Client-Available-Flash=5875028;
Client-Memory=45298688; Client-Free-Memory=6295596;
Client-Image=flash:c831-k9o3y6-mz.ef90241
```

#### Related Commands

Command	Description
<b>aaa accounting update</b>	Enables the periodic interim accounting records to be sent to the accounting server.
<b>radius-server vsa send</b>	Configures the network access server (NAS) to recognize and use vendor-specific attributes (VSAs).
<b>clear crypto session</b>	Deletes crypto sessions (IPSec and IKE) SAs.
<b>show crypto session</b>	Displays status information for active crypto sessions in a router.