show i

show idb

To display information about the status of interface descriptor blocks, which are the internal data structure representing interface resources, use the **show idb** command.

show idb

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show idb
Maximum number of Software IDBs 2252.  In use(total) 16. In use(active) 16

                    HWIDBs     SWIDBs
            Active 15         15
          Inactive 1          1
        Total IDBs 16         16
 Size each (bytes) 984        1512
       Total bytes 15744      24192

HWIDB#  1 0xdacf1420  Virtual0
HWIDB#  2 0xdac4da20  GigabitEthernet1/1
HWIDB#  3 0xdac5aa20  GigabitEthernet1/2
HWIDB#  4 0xdac651b0  GigabitEthernet1/3
HWIDB#  5 0xdac6f940  GigabitEthernet1/4
HWIDB#  6 0xdac7a0d0  GigabitEthernet1/5
HWIDB#  7 0xdac84860  GigabitEthernet1/6
HWIDB#  8 0xdac8eff0  GigabitEthernet1/7
HWIDB#  9 0xdac99780  GigabitEthernet1/8
HWIDB# 10 0xdacbda00  Internal-Control1/1
HWIDB# 11 0xdaca3f10  Internal-Data1/1
HWIDB# 12 0xdacb3260  Internal-Data1/2
HWIDB# 13 0xdacc81a0  Internal-Data1/3
HWIDB# 14 0xd409e4e0  Internal-Data1/4
HWIDB# 15 0xd409d090  Management1/1

SWIDB#  1 0xdacf1840 0x00000041 Virtual0 UP UP
SWIDB#  2 0xdac4de40 0x00000002 GigabitEthernet1/1 UP DOWN
SWIDB#  3 0xdac5ae40 0x00000003 GigabitEthernet1/2 UP DOWN
SWIDB#  4 0xdac655d0 0xffffffff GigabitEthernet1/3 DOWN DOWN
SWIDB#  5 0xdac6fd60 0xffffffff GigabitEthernet1/4 DOWN DOWN
SWIDB#  6 0xdac7a4f0 0xffffffff GigabitEthernet1/5 DOWN DOWN
SWIDB#  7 0xdac84c80 0xffffffff GigabitEthernet1/6 DOWN DOWN
SWIDB#  8 0xdac8f410 0xffffffff GigabitEthernet1/7 DOWN DOWN
SWIDB#  9 0xdac99ba0 0xffffffff GigabitEthernet1/8 DOWN DOWN
SWIDB# 10 0xdacbde20 0x0000003f Internal-Control1/1 UP UP
SWIDB# 11 0xdaca4330 0x00000043 Internal-Data1/1 UP UP
SWIDB# 12 0xdacb3680 0xffffffff Internal-Data1/2 UP UP
SWIDB# 13 0xdacc85c0 0x00000044 Internal-Data1/3 UP UP
SWIDB# 14 0xdacae210 0x00000045 Internal-Data1/4 UP UP
SWIDB# 15 0xd409d4b0 0x00000004 Management1/1 UP UP
```

The following table explains each field.

Table 1: show idb stats Fields

Field	Description
HWIDBs	Shows the statistics for all HWIDBs. HWIDBs are created for each hardware port in the system.
SWIDBs	Shows the statistics for all SWIDBs. SWIDBs are created for each main and subinterface in the system, and for each interface that is allocated to a context. Some other internal software modules also create IDBs.
HWIDB#	Specifies a hardware interface entry. The IDB sequence number, address, and interface name is displayed in each line.
SWIDB#	Specifies a software interface entry. The IDB sequence number, address, corresponding vPif id, and interface name are displayed in each line.
PEER IDB#	Specifies an interface allocated to a context. The IDB sequence number, address, corresponding vPif id, context id and interface name are displayed in each line.

Related Commands

Command	Description
show interface	Displays the runtime status and statistics of interfaces.

show identity-subnet-filter

To display the subnets excluded from receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings, use the **show identity-subnet-filter** command.

show identity-subnet-filter

Command History

Release	Modification
6.7	This command was introduced.

Usage Guidelines

The **show identity-subnet-filter** command displays all subnets currently excluded from user-to-IP and Security Group Tag (SGT)-to-IP mappings.

Examples

The following is sample output from the **show identity-subnet-filter** command if no subnets are currently excluded:

```
> show identity-subnet-filter

Subnet filter file doesn't exist
```

The following is sample output from the **show identity-subnet-filter** command if some subnets are currently excluded:

```
> show identity-subnet-filter

Subnet filters are:
2001:db8::2/64
192.0.2.0/24
```

Related Commands

Command	Description
configure identity-subnet-filter	Exclude subnets from user-to-IP and SGT-to-IP mappings.

show igmp groups

To display the multicast groups with receivers that are directly connected to the threat defense device and that were learned through IGMP, use the **show igmp groups** command.

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

Syntax Description

detail	(Optional) Provides a detailed description of the sources.
group	(Optional) The address of an IGMP group. Including this optional argument limits the display to the specified group.
if_name	(Optional) Displays group information for the specified interface.
reserved	(Optional) Displays information about reserved groups.
summary	(Optional) Displays group joins summary information.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

If you omit all optional arguments and keywords, the **show igmp groups** command displays all directly connected multicast groups by group address, interface type, and interface number.

Examples

The following is sample output from the **show igmp groups** command:

```
> show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

show igmp interface

To display multicast information for an interface, use the **show igmp interface** command.

show igmp interface [*if_name*]

Syntax Description

if_name	(Optional) Displays IGMP group information for the selected interface.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

If you omit the optional *if_name* argument, the **show igmp interface** command displays information about all interfaces.

Examples

The following is sample output from the **show igmp interface** command:

```
> show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the threat defense device and that were learned through IGMP.

show igmp traffic

To display IGMP traffic statistics, use the **show igmp traffic** command.

show igmp traffic

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                              Received     Sent
Valid IGMP Packets               3           6
Queries                          2           6
Reports                          1           0
Leaves                           0           0
Mtrace packets                   0           0
DVMRP packets                    0           0
PIM packets                      0           0

Errors:
Malformed Packets                0
Martian source                   0
Bad Checksums                    0
```

Related Commands

Command	Description
clear igmp counters	Clears all IGMP statistic counters.
clear igmp traffic	Clears the IGMP traffic counters.

show inline-set

To view information about inline sets, which are IPS-only interfaces, configured on the device, use the **show inline-set** command.

show inline-set [*inline-set-name* | **mac-address-table**]

Syntax Description

inline-set-name	(Optional) Displays information about the specified inline set. If you do not include a name, all inline sets are shown.
mac-address-table	(Optional) Displays the MAC address bridge table for the inline set.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show inline-set** command:

```
> show inline-set
Inline-set ips-inline
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: GigabitEthernet0/3 "inline-inside"
      Current-Status: UP
    Interface: GigabitEthernet0/4 "inline-outside"
      Current-Status: DOWN
    Bridge Group ID: 504
```

show interface

To view interface statistics, use the **show interface** command.

show interface [{*physical_interface* | **redundant***number*}[**.***subinterface*] | *interface_name* | **BVI** *id* |] [**summary** | **stats** | **detail**]

Syntax Description

BVI *id*	(Optional) Shows statistics for the indicated Bridge Virtual Interface (BVI). Enter the BVI number, from 1-250.
detail	(Optional) Shows detailed interface information, including the order in which the interface was added, the configured state, the actual state, and asymmetrical routing statistics, if enabled. If you show all interfaces, then you also see information about internal interfaces that are used for system communications. Internal interfaces are not user-configurable, and the information is for debugging purposes only.
interface_name	(Optional) Identifies the interface by logical name.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. The available interfaces differ by device model. Use the show interface command without parameters to see the names available on your device.
redundant*number*	(Optional) Identifies the redundant interface ID, such as **redundant1**.
stats	(Default) Shows interface information and statistics. This keyword is the default, so this keyword is optional.
summary	(Optional) Shows summary information about an interface.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Command Default

If you do not identify any options, this command shows basic statistics for all interfaces excluding internal interfaces.

Command History

Release	Modification
6.1	This command was introduced.
6.2	The **BVI** keyword was added.
6.7	Output was added to the **detail** keyword for the Internal-Data0/1 "nlp_int_tap" interface when you configure management center access on a data interface.

Usage Guidelines

The number of statistics shown for subinterfaces is a subset of the number of statistics shown for a physical interface.

Note The number of bytes transmitted or received in the Hardware count and the Traffic Statistics count are different.

In the hardware count, the amount is retrieved directly from hardware, and reflects the Layer 2 packet size. While in traffic statistics, it reflects the Layer 3 packet size.

The count difference is varied based upon the design of the interface card hardware.

For example, for a Fast Ethernet card, the Layer 2 count is 14 bytes greater than the traffic count, because it includes the Ethernet header. On the Gigabit Ethernet card, the Layer 2 count is 18 bytes greater than the traffic count, because it includes both the Ethernet header and the CRC.

See the "Examples" section for a description of the display output.

Examples

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

```
> show interface
Interface GigabitEthernet1/1 "outside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f2, MTU 1500
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
  Traffic Statistics for "outside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/2 "inside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f3, MTU 1500
        IP address 192.168.45.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
```

```
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/3 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f4, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/4 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f5, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/5 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f6, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/6 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f7, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/7 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f8, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/8 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f9, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
```

```
       input queue (blocks free curr/low): hardware (2047/2047)
       output queue (blocks free curr/low): hardware (2047/2047)
Interface Management1/1 "diagnostic", is up, line protocol is up
  Hardware is en_vtun rev00, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
       Input flow control is unsupported, output flow control is off
       MAC address e865.49b8.97f1, MTU 1500
       IP address unassigned
       14247681 packets input, 896591753 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       0 packets output, 0 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 0 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops
       input queue (blocks free curr/low): hardware (0/0)
       output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "diagnostic":
       14247685 packets input, 697121911 bytes
       0 packets output, 0 bytes
       5054964 packets dropped
     1 minute input rate 2 pkts/sec,  131 bytes/sec
     1 minute output rate 0 pkts/sec,  0 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 2 pkts/sec,  108 bytes/sec
     5 minute output rate 0 pkts/sec,  0 bytes/sec
     5 minute drop rate, 0 pkts/sec
       Management-only interface. Blocked 0 through-the-device packets
```

The following table shows each field description.

Table 2: show interface Fields

Field	Description
Interface ID	The interface ID.
"*interface_name*"	The logical interface name. If you do not configure a name, the following message appears after the Hardware line: `Available but not configured via nameif`
is *state*	The administrative state, as follows: • up—The interface is not shut down. • administratively down—The interface is shut down intentionally.
Line protocol is state	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.
VLAN identifier	For subinterfaces, the VLAN ID.

Field	Description
Hardware	The interface type, maximum bandwidth, delay, duplex, and speed. When the link is down, the duplex and speed show the configured values. When the link is up, these fields show the configured values with the actual settings in parentheses.
Media-type	(Not always shown) Shows the interface media type, such as RJ-45 or SFP.
message area	A message might be displayed in some circumstances. See the following examples: • If you do not configure a name, you see the following message: Available but not configured via nameif • If an interface is a member of a redundant interface, you see the following message: Active member of Redundant5
MAC address	The interface MAC address.
Site Specific MAC address	For clustering, shows an in-use site-specific MAC address.
MTU	The maximum size, in bytes, of packets allowed on this interface. If you do not set the interface name, this field shows “MTU not set.”
IP address	The interface IP address, either static or received from a DHCP server.
Subnet mask	The subnet mask for the IP address.
Packets input	The number of packets received on this interface.
Bytes	The number of bytes received on this interface.
No buffer	The number of failures from block allocations.
Received:	
Broadcasts	The number of broadcasts received.
Input errors	The number of total input errors, including the types listed below. Other input-related errors can also cause the input error count to increase, and some datagrams might have more than one error; therefore, this sum might exceed the number of errors listed for the types below.
Runts	The number of packets that are discarded because they are smaller than the minimum packet size, which is 64 bytes. Runts are usually caused by collisions. They might also be caused by poor wiring and electrical interference.
Giants	The number of packets that are discarded because they exceed the maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.

Field	Description
CRC	The number of Cyclical Redundancy Check errors. When a station sends a frame, it appends a CRC to the end of the frame. This CRC is generated from an algorithm based on the data in the frame. If the frame is altered between the source and destination, the system notes that the CRC does not match. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Frame	The number of frame errors. Bad frames include packets with an incorrect length or bad frame checksums. This error is usually the result of collisions or a malfunctioning Ethernet device.
Overrun	The number of times that the interface was incapable of handing received data to a hardware buffer because the input rate exceeded the interface's capability to handle the data.
Ignored	This field is not used. The value is always 0.
Abort	This field is not used. The value is always 0.
L2 decode drops	The number of packets dropped because the name is not configured or a frame with an invalid VLAN id is received. On a standby interface in a redundant interface configuration, this counter may increase because this interface has no name configured.
Packets output	The number of packets sent on this interface.
Bytes	The number of bytes sent on this interface.
Underruns	The number of times that the transmitter ran faster than the interface could handle.
Output Errors	The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.
Collisions	The number of messages retransmitted due to an Ethernet collision (single and multiple collisions). This usually occurs on an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once by the output packets.
Interface resets	The number of times an interface has been reset. If an interface is unable to transmit for three seconds, the system resets the interface to restart transmission. During this interval, connection state is maintained. An interface reset can also happen when an interface is looped back or shut down.
Babbles	Unused. ("babble" means that the transmitter has been on the interface longer than the time taken to transmit the largest frame.)

Field	Description
Late collisions	The number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait. If you get a late collision, a device is jumping in and trying to send the packet on the Ethernet while the threat defense device is partly finished sending the packet. The threat defense device does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks and Ethernet networks running beyond the specification.
Deferred	The number of frames that were deferred before transmission due to activity on the link.
input reset drops	Counts the number of packets dropped in the RX ring when a reset occurs.
output reset drops	Counts the number of packets dropped in the TX ring when a reset occurs.
Rate limit drops	The number of packets dropped if you configured the interface at non-Gigabit speeds and attempted to transmit more than 10 Mbps or 100 Mbps, depending on configuration..
Lost carrier	The number of times the carrier signal was lost during transmission.
No carrier	Unused.
Input queue (curr/max packets):	The number of packets in the input queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue. Not available for Gigabit Ethernet interfaces.
Output queue (curr/max packets):	The number of packets in the output queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue.
input queue (blocks free curr/low)	The curr/low entry indicates the number of current and all-time-lowest available slots on the interface's Receive (input) descriptor ring. These are updated by the main CPU, so the all-time-lowest (until the interface statistics are cleared or the device is reloaded) watermarks are not highly accurate.

Field	Description
output queue (blocks free curr/low)	The curr/low entry indicates the number of current and all-time-lowest available slots on the interface's Transmit (output) descriptor rings. These are updated by the main CPU, so the all-time-lowest (until the interface statistics are cleared or the device is reloaded) watermarks are not highly accurate.
Traffic Statistics:	The number of packets received, transmitted, or dropped.
Packets input	The number of packets received and the number of bytes.
Packets output	The number of packets transmitted and the number of bytes.
Packets dropped	The number of packets dropped. Typically this counter increments for packets dropped on the accelerated security path (ASP), for example, if a packet is dropped due to an access list deny. See the **show asp drop** command for reasons for potential drops on an interface.
1 minute input rate	The number of packets received in packets/sec and bytes/sec over the last minute.
1 minute output rate	The number of packets transmitted in packets/sec and bytes/sec over the last minute.
1 minute drop rate	The number of packets dropped in packets/sec over the last minute.
5 minute input rate	The number of packets received in packets/sec and bytes/sec over the last 5 minutes.
5 minute output rate	The number of packets transmitted in packets/sec and bytes/sec over the last 5 minutes.
5 minute drop rate	The number of packets dropped in packets/sec over the last 5 minutes.
Redundancy Information:	For redundant interfaces, shows the member physical interfaces. The active interface has "(Active)" after the interface ID. If you have not yet assigned members, you see the following output: `Members unassigned`
Last switchover	For redundant interfaces, shows the last time the active interface failed over to the standby interface.

Note The input and output rates in the **show interface detail** command result can be different from the input and output traffic rates that appear in the interface module of the management center user interface.

The interface module displays the traffic rates according to the values from Snort performance monitoring. Sampling intervals of snort performance monitoring and the interface statistics are different. This difference in sampling intervals results in different throughput values in the management center user interface and in the **show interface detail** command result.

The following is sample output from the **show interface detail** command. The following example shows detailed interface statistics for all interfaces, including the internal interfaces (if present for your platform) and asymmetrical routing statistics, if enabled:

```
> show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
```

```
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
[...]
```

The following table explains the additional fields shown by the **show interface detail** command.

Table 3: show interface detail Fields

Field	Description
Demux drops	(On Internal-Data interface only) The number of packets dropped because the threat defense device was unable to demultiplex packets from other interfaces.
Control Point Interface States:	
Interface number	A number used for debugging that indicates in what order this interface was created, starting with 0.
Interface config status	The administrative state, as follows: • active—The interface is not shut down. • not active—The interface is shut down intentionally.
Interface state	The actual state of the interface. In most cases, this state matches the config status above. If you configure high availability, it is possible there can be a mismatch because the threat defense device brings the interfaces up or down as needed.
Asymmetrical Routing Statistics:	
Received X1 packets	Number of ASR packets received on this interface.
Transmitted X2 packets	Number of ASR packets sent on this interfaces.
Dropped X3 packets	Number of ASR packets dropped on this interface. The packets might be dropped if the interface is down when trying to forward the packet.

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
show interface ip brief	Shows the interface IP address and status.

show interface ip brief

To view interface IP addresses and status, use the **show interface ip brief** command.

show interface [[*physical_interface*[**.***subinterface*] | *interface_name* | **BVI** *id* |] **ip brief**

Syntax Description

BVI *id*	(Optional) Shows statistics for the indicated Bridge Virtual Interface (BVI). Enter the BVI number, from 1-250.
interface_name	(Optional) Identifies the interface name.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Command Default

If you do not specify an interface, the command shows all interfaces, including internal interfaces.

Command History

Release	Modification
6.1	This command was introduced.
6.2	The **BVI** keyword was added.

Examples

The following is sample output from the **show ip brief** command:

```
> show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   administratively down down
    GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
    Management0/0              209.165.201.3   YES CONFIG  up
```

The following example shows addressing when most interfaces are part of a BVI. The member interfaces have the same address as the parent BVI.

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet1/1         unassigned      YES DHCP   down                  down
GigabitEthernet1/2         192.168.1.1     YES unset  down                  down
GigabitEthernet1/3         192.168.1.1     YES unset  down                  down
GigabitEthernet1/4         192.168.1.1     YES unset  down                  down
GigabitEthernet1/5         192.168.1.1     YES unset  down                  down
GigabitEthernet1/6         192.168.1.1     YES unset  down                  down
GigabitEthernet1/7         192.168.1.1     YES unset  down                  down
GigabitEthernet1/8         192.168.1.1     YES unset  down                  down
Internal-Control1/1        127.0.1.1       YES unset  up                    up
Internal-Data1/1           unassigned      YES unset  up                    up
```

```
Internal-Data1/2           unassigned      YES unset  down                  down
Internal-Data1/3           unassigned      YES unset  up                    up
Internal-Data1/4           169.254.1.1     YES unset  up                    up
Management1/1              unassigned      YES unset  up                    up
BVI1                       192.168.1.1     YES manual up                    up
```

The following table explains the output fields.

Table 4: show interface ip brief Fields

Field	Description
Interface	The interface ID. If you show all interfaces, then you also see information about internal interfaces that are used for system communications. Internal interfaces are not user-configurable, and the information is for debugging purposes only.
IP-Address	The interface IP address.
OK?	This column is not used, and always shows “Yes.”
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—The interface has a static address. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.
Status	The administrative state, as follows: • up—The interface is not shut down. • down—The interface is not up, nor is it intentionally shut down. • administratively down—The interface is shut down intentionally.
Protocol	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.

Related Commands

Command	Description
show interface	Displays the runtime status and statistics of interfaces.

show inventory

To display information about all of the Cisco products installed in the networking device that are assigned a product identifier (PID), version identifier (VID), and serial number (SN), use the **show inventory** command.

show inventory [*slot_id*]

Syntax Description

slot_id	(Optional) Specifies the module ID or slot number, 0-3.

Command Default

If you do not specify a slot to show inventory for an item, the inventory information of all modules (including the power supply) is displayed.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a UDI, which is a combination of three separate data elements: the product identifier (PID), the version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the “Product Name” or “Part Number.” This is the identifier that you use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product has a unique serial number assigned at the factory, which cannot be changed in the field. The serial number is the means by which to identify an individual, specific instance of a product. The serial number can be different lengths for the various components of the device.

The UDI refers to each product as an entity. Some entities, such as a chassis, have sub-entities like slots. Each entity appears on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the **show inventory** command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

If a Cisco entity is not assigned a PID, that entity is not retrieved or displayed.

The serial number may not display because of hardware limitations on the ASA 5500-X series. For the UDI display of the PCI-E I/O (NIC) option cards in these models, there are six possible outputs according to the chassis type, although there are only two different card types. This is because there are different PCI-E bracket assemblies used according to the specified chassis. The following examples show the expected outputs for each PCI-E I/O card assembly. For example, if a Silicom SFP NIC card is detected, the UDI display is determined by the device on which it is installed. The VID and S/N values are N/A, because there is no electronic storage of these values.

For a 6-port SFP Ethernet NIC card in an ASA 5512-X or 5515-X:

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
```

```
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

For a 6-port SFP Ethernet NIC card in an ASA 5525-X:

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

For a 6-port SFP Ethernet NIC card in an ASA 5545-X or 5555-X:

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

For a 6-port Copper Ethernet NIC card in an ASA 5512-X or 5515-X:

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

For a 6-port Copper Ethernet NIC card in an ASA 5525-X:

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

For a 6-port Copper Ethernet NIC card in an ASA 5545-X or 5555-X:

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

Examples

The following is sample output from the **show inventory** command without any keywords or arguments. This sample output displays a list of Cisco entities installed in an threat defense device that are each assigned a PID.

```
> show inventory
Name: "Chassis", DESCR: "ASA 5508-X with FirePOWER services, 8GE, AC, DES"
PID: ASA5508           , VID: V01     , SN: JMX1923408S

Name: "Storage Device 1", DESCR: "ASA 5508-X SSD"
PID: ASA5508-SSD       , VID: N/A     , SN: MXA184205MC
```

The following table describes the fields shown in the display.

Table 5: Field Descriptions for show inventory

Field	Description
Name	Physical name (text string) assigned to the Cisco entity. For example, console, SSP, or a simple component number (port or module number), such as “1,” depending on the physical component naming syntax of the device. Equivalent to the entPhysicalName MIB variable in RFC 2737.

Field	Description
DESCR	Physical description of the Cisco entity that characterizes the object. Equivalent to the entPhysicalDesc MIB variable in RFC 2737.
PID	Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.
VID	Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.
SN	Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.

show ip address

To view interface IP addresses or, for transparent mode, the management IP address, use the **show ip address** command.

show ip address [[*physical_interface*[**.***subinterface*] | *interface_name* |]

Syntax Description

interface_name	(Optional) Identifies the interface name.
physical_interface	(Optional) Identifies the interface ID, such as **gigabit**ethernet0/1.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Command Default

If you do not specify an interface, the output shows all interface IP addresses.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command shows the primary IP addresses (called "System" in the display) for when you configure high availability as well as the current IP addresses. If the unit is active, then the system and current IP addresses match. If the unit is standby, then the current IP addresses show the standby addresses.

The IP addresses are for data interfaces only. This command does not show the system's IP address on the management interface on the diagnotic interface (which is not the same as a transparent mode management interface). The information will include IP address information for the diagnostic interface, if one is configured. To see information about the management interface, use the **show network** command.

Examples

The following is sample output from the **show ip address** command:

```
> show ip address
System IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
```

The following table explains each field.

Table 6: show ip address Fields

Field	Description
Interface	The interface ID.
Name	The interface name.
IP address	The interface IP address.
Subnet mask	The IP address subnet mask.
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—The interface has a static address. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.

Related Commands

Command	Description
show interface	Displays the runtime status and statistics of interfaces.
show interface ip brief	Shows the interface IP address and status.

show ip address dhcp

To view detailed information about the DHCP lease or server for an interface, use the **show ip address dhcp** command.

show ip address {*physical_interface*[**.***subinterface*] | *interface_name*} **dhcp server**
show ip address {*physical_interface*[**.***subinterface*] | *interface_name*} **dhcp lease** [**proxy** | **server**] [**summary**]

Syntax Description

interface_name	Identifies the interface name.
lease	Shows information about the DHCP lease.
physical_interface	Identifies the interface ID, such as **gigabitethernet0/1**.
proxy	Shows proxy entries in the IPL table.
server	Shows server entries in the IPL table.
subinterface	Identifies an integer between 1 and 4294967293 designating a logical subinterface.
summary	Shows summary for the entry.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show ip address dhcp lease** command:

```
> show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

The following table explains each field.

Table 7: show ip address dhcp lease Fields

Field	Description
Temp IP Addr	The IP address assigned to the interface.

Field	Description
Temp sub net mask	The subnet mask assigned to the interface.
DHCP Lease server	The DHCP server address.
state	The state of the DHCP lease, as follows: • Initial—The initialization state, where the device begins the process of acquiring a lease. This state is also shown when a lease ends or when a lease negotiation fails. • Selecting—The device is waiting to receive DHCPOFFER messages from one or more DHCP servers, so it can choose one. • Requesting—The device is waiting to hear back from the server to which it sent its request. • Purging—The device is removing the lease because the client has released the IP address or there was some other error. • Bound—The device has a valid lease and is operating normally. • Renewing—The device is trying to renew the lease. It regularly sends DHCPREQUEST messages to the current DHCP server, and waits for a reply. • Rebinding—The device failed to renew the lease with the original server, and now sends DHCPREQUEST messages until it gets a reply from any server or the lease ends. • Holddown—The device started the process to remove the lease. • Releasing—The device sends release messages to the server indicating that the IP address is no longer needed.
DHCP transaction id	A random number chosen by the client, used by the client and server to associate the request messages.
Lease	The length of time, specified by the DHCP server, that the interface can use this IP address.
Renewal	The length of time until the interface automatically attempts to renew this lease.
Rebind	The length of time until the threat defense device attempts to rebind to a DHCP server. Rebinding occurs if the device cannot communicate with the original DHCP server, and 87.5 percent of the lease time has expired. The device then attempts to contact any available DHCP server by broadcasting DHCP requests.
Temp default-gateway addr	The default gateway address supplied by the DHCP server.
Temp ip static route0	The default static route.
Next timer fires after	The number of seconds until the internal timer triggers.

Field	Description
Retry count	If the threat defense device is attempting to establish a lease, this field shows the number of times the device tried sending a DHCP message. For example, if the device is in the Selecting state, this value shows the number of times the device sent discover messages. If the device is in the Requesting state, this value shows the number of times the device sent request messages.
Client-ID	The client ID used in all communication with the server.
Proxy	Specifies if this interface is a proxy DHCP client for VPN clients, True or False.
Proxy Network	The requested network.
Hostname	The client hostname.

The following is sample output from the **show ip address dhcp server** command:

```
> show ip address outside dhcp server
   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

The following table explains each field.

Table 8: show ip address dhcp server Fields

Field	Description
DHCP server	The DHCP server address from which this interface obtained a lease. The top entry (“ANY”) is the default server and is always present.
Leases	The number of leases obtained from the server. For an interface, the number of leases is typically 1. If the server is providing address for an interface that is running proxy for VPN, there will be several leases.
Offers	The number of offers from the server.
Requests	The number of requests sent to the server.
Acks	The number of acknowledgments received from the server.
Naks	The number of negative acknowledgments received from the server.
Declines	The number of declines received from the server.
Releases	The number of releases sent to the server.

Field	Description
Bad	The number of bad packets received from the server.
DNS0	The primary DNS server address obtained from the DHCP server.
DNS1	The secondary DNS server address obtained from the DHCP server.
WINS0	The primary WINS server address obtained from the DHCP server.
WINS1	The secondary WINS server address obtained from the DHCP server.
Subnet	The subnet address obtained from the DHCP server.
DNS Domain	The domain obtained from the DHCP server.

Related Commands

Command	Description
show interface ip brief	Shows the interface IP address and status.
show ip address	Displays the IP addresses of interfaces.

show ip address pppoe

To view detailed information about the PPPoE connection, use the **show ip address pppoe** command.

show ip address {*physical_interface*[**.***subinterface*] | *interface_name* | } **pppoe**

Syntax Description

interface_name	Identifies the interface name.
physical_interface	Identifies the interface ID, such as **gigabitethernet0/1**.
subinterface	Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Command History

Release	Modification
6.1	This command was introduced.

Related Commands

Command	Description
show interface ip brief	Shows the interface IP address and status.
show ip address	Displays the IP addresses of interfaces.

show ip audit count

To show the number of signature matches when you apply an audit policy to an interface, use the **show ip audit count** command.

show ip audit count [**global** | **interface** *interface_name*]

Syntax Description

global	(Default) Shows the number of matches for all interfaces.
interface *interface_name*	(Optional) Shows the number of matches for the specified interface.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The audit policy is normally not configured, but if you configure it using a FlexConfig, you can view the related statistics.

Related Commands

Command	Description
clear ip audit count	Clears the statistics for IP audit.
show running-config ip audit name	Shows the configuration for the **ip audit name** command. Besides **name**, you can check on the **interface** and **signature** configuration.

show ip local pool

To display IPv4 address pool information, use the **show ip local pool** command.

show ip local pool *pool_name*

Syntax Description

pool_name	The name of an IPv6 address pool.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to view the contents of IPv4 address pools. These pools are used with remote access VPN and clustering. Use **show ipv6 local pool** to view IPv6 address pools.

Examples

The following is sample output from the **show ip local pool** command:

```
> show ip local pool test-ipv4-pool
Begin           End             Mask            Free     Held     In use
10.100.10.10    10.100.10.254   255.255.255.0     245        0        0

Available Addresses:
10.100.10.10
10.100.10.11
10.100.10.12
10.100.10.13
10.100.10.14
10.100.10.15
10.100.10.16
... (remaining output redacted)...
```

show ip verify statistics

To show the number of packets dropped because of the Unicast Reverse Path Forwarding (RPF) feature, use the **show ip verify statistics** command.

show ip verify statistics [**interface** *interface_name*]

Syntax Description

interface *interface_name*	(Optional) Shows statistics for the specified interface.

Command Default

This command shows statistics for all interfaces.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **ip verify reverse-path** feature is normally not configured, but if you configure it using a FlexConfig, you can view the related statistics.

Examples

The following is sample output from the **show ip verify statistics** command:

```
> show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

Related Commands

Command	Description
clear ip verify statistics	Clears the Unicast RPF statistics.
show running-config ip verify reverse-path	Shows the **ip verify reverse-path** configuration.

show ipsec df-bit

To display the IPsec do-not-fragment (DF-bit) policy for IPsec packets for a specified interface, use the **show ipsec df-bit** command. You can also use the command synonym **show crypto ipsec df-bit**.

show ipsec df-bit *interface*

Syntax Description

interface	Specifies an interface name.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The df-bit setting determines how the system handles the do-not-fragment (DF) bit in the encapsulated header. The DF bit within the IP header determines whether or not a device is allowed to fragment a packet. Based on this setting, the system either clears, sets, or copies the DF-bit setting of the clear-text packet to the outer IPsec header when applying encryption.

Examples

The following example displays the IPsec DF-bit policy for interface named inside:

```
> show ipsec df-bit inside
df-bit inside copy
```

Related Commands

Command	Description
show ipsec fragmentation	Displays the fragmentation policy for IPsec packets.

show ipsec fragmentation

To display the fragmentation policy for IPsec packets, use the **show ipsec fragmentation** command. You can also use the command synonym **show crypto ipsec fragmentation**.

show ipsec fragmentation *interface*

Syntax Description

interface	Specifies an interface name.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

When encrypting packets for a VPN, the system compares the packet length with the MTU of the outbound interface. If encrypting the packet will exceed the MTU, the packet must be fragmented. This command shows whether the system will fragment the packet after encrypting it (after-encryption), or before encrypting it (before-encryption). Fragmenting the packet before encryption is also called prefragmentation, and is the default system behavior because it improves overall encryption performance.

Examples

The following example displays the IPsec fragmentation policy for an interface named inside:

```
> show ipsec fragmentation inside
fragmentation inside before-encryption
```

Related Commands

Command	Description
show ipsec df-bit	Displays the DF-bit policy for a specified interface.

show ipsec policy

To display IPsec secure socket API (SS API) security policy configure for OSPFv3, use the **show ipsec policy** command. You can also use the alternate form of this command: **show crypto ipsec policy**.

show ipsec policy

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example shows the OSPFv3 authentication and encryption policy.

```
> show ipsec policy
Crypto IPsec client security policy data

Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901
Outbound ESP Auth Key:   12345678901234567890123456789012345678901
Inbound  ESP Cipher Key: 123456789012345678901234567890123456789012
Outbound ESP Cipher Key: 123456789012345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

Related Commands

Command	Description
show crypto sockets	Displays secure socket information.
show ipv6 ospf interface	Displays information about OSPFv3 interfaces.

show ipsec sa

To display a list of IPsec security associations (SAs), use the **show ipsec sa** command. You can also use the alternate form of this command: **show crypto ipsec sa**.

show ipsec sa [**assigned-address** *hostname_or_IP_address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr* | **spi** *spi-num*] [**detail**]

Syntax Description

assigned-address *hostname_or_IP_address*	(Optional) Displays IPsec SAs for the specified hostname or IP address.
detail	(Optional) Displays detailed error information on what is displayed.
entry	(Optional) Displays IPsec SAs sorted by peer address
identity	(Optional) Displays IPsec SAs for sorted by identity, not including ESPs. This is a condensed form.
inactive	(Optional) Displays IPsec SAs that are unable to pass traffic.
map *map-name*	(Optional) Displays IPsec SAs for the specified crypto map.
peer *peer-addr*	(Optional) Displays IPsec SAs for specified peer IP addresses.
spi *spi-num*	(Optional) Displays IPsec SAs for an SPI.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example displays IPsec SAs, including the assigned IPv6 address and the Transport Mode and GRE encapsulation indication.

```
> show ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

```
      #send errors: 0, #recv errors: 4

     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

The following example displays IPsec SAs, including an in-use setting to identify a tunnel as OSPFv3.

```
> show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3),}
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
```

```
    spi: 0xDC15BF68 (3692412776)
       transform: esp-3des esp-md5-hmac
       in use settings ={L2L, Transport, Manual key (OSPFv3), }
       slot: 0, conn_id: 3, crypto-map: def
       sa timing: remaining key lifetime (sec): 548
       IV size: 8 bytes
       replay detection support: Y

  Crypto map tag: def, local addr: 10.132.0.17

    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

Note Fragmentation statistics are pre-fragmentation statistics if the IPsec SA policy states that fragmentation occurs before IPsec processing. Post-fragmentation statistics appear if the SA policy states that fragmentation occurs after IPsec processing.

The following example, entered in global configuration mode, displays IPsec SAs for a crypto map named def.

```
> show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17
```

```
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
    current_peer: 10.135.1.8
    dynamic allocated peer ip: 0.0.0.0

    #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
    #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: 3B6F6A35

  inbound esp sas:
    spi: 0xB32CF0BD (3006066877)
       transform: esp-3des esp-md5-hmac
       in use settings ={RA, Tunnel, }
       slot: 0, conn_id: 4, crypto-map: def
       sa timing: remaining key lifetime (sec): 263
       IV size: 8 bytes
       replay detection support: Y
  outbound esp sas:
    spi: 0x3B6F6A35 (997157429)
       transform: esp-3des esp-md5-hmac
       in use settings ={RA, Tunnel, }
       slot: 0, conn_id: 4, crypto-map: def
       sa timing: remaining key lifetime (sec): 263
       IV size: 8 bytes
       replay detection support: Y
```

The following example shows IPsec SAs for the keyword **entry**.

```
> show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
```

```
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
```

The following example shows IPsec SAs with the keywords **entry detail**.

```
> show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp 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

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp 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

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
```

```
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
>
```

The following example shows IPsec SAs with the keyword **identity**.

```
> show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

The following example shows IPsec SAs with the keywords **identity** and **detail**.

```
> show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp 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

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp 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

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

The following example displays IPSec SAs based on IPv6 assigned address:

```
> show ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 35

      local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
```

```
  current inbound spi : 4FCB6624

inbound esp sas:
  spi: 0x4FCB6624 (1338730020)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
  spi: 0xD9C00FC2 (3653242818)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
```

Related Commands

Command	Description
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active ISAKMP configuration.

show ipsec sa summary

To display a summary of IPsec SAs, use the **show ipsec sa summary** command.

show ipsec sa summary

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example displays a summary of IPsec SAs by the following connection types:

- IPsec
- IPsec over UDP
- IPsec over NAT-T
- IPsec over TCP
- IPsec VPN load balancing

```
> show ipsec sa summary
Current IPsec SA's:           Peak IPsec SA's:
IPsec            :     2        Peak Concurrent SA  :    14
IPsec over UDP   :     2        Peak Concurrent L2L :     0
IPsec over NAT-T :     4        Peak Concurrent RA  :    14
IPsec over TCP   :     6
IPsec VPN LB     :     0
Total            :    14
```

Related Commands

Command	Description
clear ipsec sa	Removes IPsec SAs entirely or based on specific parameters.
show ipsec sa	Displays a list of IPsec SAs.
show ipsec stats	Displays a list of IPsec statistics.

show ipsec stats

To display a list of IPsec statistics, use the **show ipsec stats** command.

show ipsec stats

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The following table describes what the output entries indicate.

Output (continued)	Description (continued)
IPsec Global Statistics	This section pertains to the total number of IPsec tunnels that the threat defense device supports.
Active tunnels	The number of IPsec tunnels that are currently connected.
Previous tunnels	The number of IPsec tunnels that have been connected, including the active ones.
Inbound	This section pertains to inbound encrypted traffic that is received through IPsec tunnels.
Bytes	The number of bytes of encrypted traffic that has been received.
Decompressed bytes	The number of bytes of encrypted traffic that were received after decompression was performed, if applicable. This counter should always be equal to the previous one if compression is not enabled.
Packets	The number of encrypted IPsec packets that were received.
Dropped packets	The number of encrypted IPsec packets that were received and dropped because of errors.
Replay failures	The number of anti-replay failure that were detected on received, encrypted IPsec packets.
Authentications	The number of successful authentications performed on received, encrypted IPsec packets.
Authentication failures	The number of authentications failure detected on received, encrypted IPsec packets.
Decryptions	The number of successful decryptions performed on received, encrypted IPsec packets.
Decryption failures	The number of decryptions failures detected on received, encrypted IPsec packets.

Output (continued)	Description (continued)
Decapsulated fragments needing reassembly	The number of decryption IPsec packets that include IP fragments to be reassembled.
Outbound	This section pertains to outbound cleartext traffic to be transmitted through IPsec traffic.
Bytes	The number of bytes of cleartext traffic to be encrypted and transmitted through IPsec tunnels.
Uncompressed bytes	The number of bytes of uncompressed cleartext traffic to be encrypted and transmitted through IPsec tunnels. The counter should always be equal to the previous one if compression is not enabled
Packets	The number of cleartext packets to be encrypted and transmitted through IPsec tunnels.
Dropped packets	The number of cleartext packets to be encrypted and transmitted through IPsec tunnels that have been dropped because of errors.
Authentications	The number of successful authentications performed on packets to be transmitted through IPsec tunnels.
Authentication failures	The number of authentication failures that were detected on packets to be transmitted through IPsec tunnels.
Encryptions	The number of successful encryptions that were performed on packets to be transmitted through IPsec tunnels.
Encryption failures	The number of encryption failures that were detected on packets to be transmitted through IPsec tunnels.
Fragmentation successes	The number of successful fragmentation operations that were performed as part of outbound IPsec packet transformation.
Pre-fragmentation successes	The number of successful prefragmentation operations that were performed as part of outbound IPsec packet transformation. Prefragmentation occurs before the cleartext packet is encrypted and encapsulated as one or more IPsec packets.
Post-fragmentation successes	The number of successful prefragmentation operations that were performed as part of outbound IPsec packet transformation. Post-fragmentation occurs after the cleartext packet is encrypted and encapsulated as an IPsec packet, which results in multiple IP fragments. These fragments must be reassembled before decryption.
Fragmentation failures	The number of fragmentation failures that have occurred during outbound IPsec packet transformation.
Pre-fragmentation failures	The number of prefragmentation failures that have occurred during outbound IPsec packet transformation. Prefragmentation occurs before the cleartext packet is encrypted and encapsulated as one or more IPsec packets.

Output (continued)	Description (continued)
Post-fragmentation failure	The number of post-fragmentation failure that have occurred during outbound IPsec packet transformation. Post-fragmentation occurs after the cleartext packet is encrypted and encapsulated as an IPsec packet, which results in multiple IP fragments. These fragments must be reassembled before decryption.
Fragments created	The number of fragments that were created as part of IPsec transformation.
PMTUs sent	The number of path MTU messages that were sent by the IPsec system. IPsec will send a PMTU message to an inside host that is sending packets that are too large to be transmitted through an IPsec tunnel after encapsulation. The PMTU message is a request for the host to lower its MTU and send smaller packets for transmission through the IPsec tunnel.
PMTUs recvd	The number of path MTU messages that were received by the IPsec system. IPsec will receive a path MTU message from a downstream network element if the packets it is sending through the tunnel are too large to traverse that network element. IPsec will usually lower its tunnel MTU when a path MTU message is received.
Protocol failures	The number of malformed IPsec packets that have been received.
Missing SA failures	The number of IPsec operations that have been requested for which the specified IPsec security association does not exist.
System capacity failures	The number of IPsec operations that cannot be completed because the capacity of the IPsec system is not high enough to support the data rate.

Examples

The following example, entered in global configuration mode, displays IPsec statistics:

```
> show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
```

```
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
```

On platforms that support IPsec flow offload, the output shows the counters for offloaded flows, and the regular counters show the total of offloaded and non-offloaded flows.

```
> show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 1
Previous tunnels: 1
Inbound
    Bytes: 93568
    Decompressed bytes: 0
    Packets: 86
    Dropped packets: 0
    Replay failures: 0
    Authentications: 0
    Authentication failures: 0
    Decryptions: 86
    Decryption failures: 0
    TFC Packets: 0
    Decapsulated fragments needing reassembly: 0
    Valid ICMP Errors rcvd: 0
    Invalid ICMP Errors rcvd: 0
Outbound
    Bytes: 93568
    Uncompressed bytes: 90472
    Packets: 86
    Dropped packets: 0
    Authentications: 0
    Authentication failures: 0
    Encryptions: 86
    Encryption failures: 0
    TFC Packets: 0
    Fragmentation successes: 0
        Pre-fragmentation successes: 0
        Post-fragmentation successes: 0
    Fragmentation failures: 0
        Pre-fragmentation failures: 0
        Post-fragmentation failures: 0
    Fragments created: 0
    PMTUs sent: 0
    PMTUs rcvd: 0
```

```
Offloaded Inbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Decryptions: 86
Offloaded Outbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Encryptions: 86
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
Inbound SA delete requests: 0
Outbound SA delete requests: 0
Inbound SA destroy calls: 0
Outbound SA destroy calls: 0
```

Related Commands

Command	Description
clear ipsec sa	Clears IPsec SAs or counters based on specified parameters.
show ipsec sa	Displays IPsec SAs based on specified parameters.
show ipsec sa summary	Displays a summary of IPsec SAs.

show ipv6 access-list

This command is for a feature that is not supported by threat defense. IPv6 access control is integrated into the standard access control policy. View the policy in the manager, or use the following commands:

- **show access-list**
- **show access-control-config**

show ipv6 dhcp

To show DHCPv6 information, use the **show ipv6 dhcp** command.

show ipv6 dhcp [**client** [**pd**] **statistics** | **interface** [*interface_name* [**statistics**]] | **ha statistics** | **server statistics** | **pool** [*pool_name*]]

Syntax Description

client [**pd**] **statistics**	Shows DHCPv6 client statistics and shows the output of the number of messages sent and received. Add the **pd** keyword to show DHCPv6 Prefix Delegation client statistics.
interface [*interface_name* [**statistics**]]	Shows DHCPv6 information for all interfaces, or optionally, the specified interface. If the interface is configured for DHCPv6 stateless server configuration, this command lists the DHCPv6 pool that is being used by the server. If the interface has DHCPv6 address client or Prefix Delegation client configuration, this command shows the state of each client and the values received from the server. If you specify the interface name, you can add **statistics** to view the message statistics for the DHCP server or client for that interface.
ha statistics	Shows the transaction statistics between failover units, including how many times the DUID information was synced between the units.
server statistics	Shows the DHCPv6 stateless server statistics.
pool [*pool_name*]	Shows all DHCPv6 pools or optionally, the specified pool.

Command History

Release	Modification
6.2.1	This command was introduced.

Usage Guidelines

If you do not specify any arguments, this command displays the device DUID that is being used by the DHCPv6 client or server.

Example

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

```
> show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00030001377E8FD91020
```

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

```
> show ipv6 dhcp pool
DHCPv6 pool: Sample-Pool
  Imported DNS server: 2004:abcd:abcd:abcd::2
  Imported DNS server: 2004:abcd:abcd:abcd::4
  Imported Domain name: relay.com
  Imported Domain name: server.com
```

```
  SIP server address: 2001::abcd:1
  SIP server domain name: sip.xyz.com
```

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

```
> show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0
```

The following is sample output from the **show ipv6 dhcp interface outside** command:

```
> show ipv6 dhcp interface outside
GigabitEthernet1/2 is in client mode


 Prefix State is OPEN
 Renew will be sent in 00:02:05
 Address State is OPEN
 Renew for address will be sent in 00:02:06
 List of known servers:
   Reachable via address: fe80::20c:29ff:fe96:1bf4
   DUID: 000100011D9D1712005056A07E06
```

```
   Preference: 0
   Configuration parameters:
     IA PD: IA ID 0x00030001, T1 250, T2 400
       Prefix: 2005:abcd:ab03::/48
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     IA NA: IA ID 0x00030001, T1 250, T2 400
       Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     DNS server: 2004:abcd:abcd:abcd::2
     DNS server: 2004:abcd:abcd:abcd::4
     Domain name: relay.com
     Domain name: server.com
     Information refresh time: 0
 Prefix name: Sample-PD
```

The following is sample output from the **show ipv6 dhcp interface outside statistics** command:

```
> show ipv6 dhcp interface outside statistics
DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

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

```
> show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0
```

The following is sample output from the **show ipv6 dhcp client pd statistics** command:

```
> show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:


 Total number of Re-transmission messages sent:                  1
 Total number of Message Validation errors in received messages: 0
```

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

```
> show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                   10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
```

```
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

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

```
> show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

The following is sample output from the **show ipv6 dhcp ha statistics** command on a standby unit:

```
> show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

Related Commands

Command	Description
clear ipv6 dhcp	Clears the DHCPv6 statistics.

show ipv6 dhcprelay binding

To display the relay binding entries created by the relay agent, use the **show ipv6 dhcprelay binding** command.

show ipv6 dhcprelay binding

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 dhcprelay binding
1 in use, 2 most used

Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds

Above binding is created for client with link local address of fe80::204:23ff:febb:b094 on
the inside interface using DHCPv6 id of 000100010f9a59d1000423bbb094, and will timeout in
60 seconds.

There will be limit of 1000 bindings for each context.
```

Related Commands

Command	Description
show ipv6 dhcprelay statistics	Shows the IPv6 DHCP relay agent information.

show ipv6 dhcprelay statistics

To display the IPv6 DHCP relay agent statistics, use the **show ipv6 dhcprelay statistics** command.

show ipv6 dhcprelay statistics

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 dhcprelay statistics
Relay Messages:
  SOLICIT                                     1
  ADVERTISE                                   2
  REQUEST                                     1
  CONFIRM                                     1
  RENEW                                     496
  REBIND                                      0
  REPLY                                     498
  RELEASE                                     0
  DECLINE                                     0
  RECONFIGURE                                 0
  INFORMATION-REQUEST                         0
  RELAY-FORWARD                             499
  RELAY-REPLY                               500

Relay Errors:
  Malformed message:                          0
  Block allocation/duplication failures:      0
  Hop count limit exceeded:                   0
  Forward binding creation failures:          0
  Reply binding lookup failures:              0
  No output route:                            0
  Conflict relay server route:                0
  Failed to add server NP rule:               0
  Unit or context is not active:              0

Total Relay Bindings Created:               498
```

Related Commands

Command	Description
show ipv6 dhcprelay binding	Shows the relay binding entries created by the relay agent.

show ipv6 general-prefix

To display the IPv6 general prefixes, use the **show ipv6 general-prefix** command.

show ipv6 general-prefix

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use the **show ipv6 general-prefix** command to view information on IPv6 general prefixes.

Examples

The following is sample output from the **show ipv6 general-prefix** command:

```
> show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
 Loopback42 (Address command)
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 icmp

To display the ICMPv6 access rules configured on all interfaces, use the **show ipv6 icmp** command.

show ipv6 icmp

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

ICMPv6 rules control ICMPv6 traffic to device interfaces. They do not control through-the-box traffic. You would use these rules to control which addresses could send ICMPv6 commands to an interface (for example, pings), and which types of ICMPv6 commands could be sent. Use the **show ipv6 icmp** command to view these rules.

Examples

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

```
> show ipv6 icmp
ipv6 icmp permit any inside
```

show ipv6 interface

To display the status of interfaces configured for IPv6, use the **show ipv6 interface** command.

show ipv6 interface [**brief**] [*if_name* [**prefix**]]

Syntax Description

brief	Displays a brief summary of IPv6 status and configuration for each interface.
if_name	(Optional) The internal or external interface name. The status and configuration for only the designated interface is shown. If you show all interfaces, then you also see information about internal interfaces that are used for system communications. Internal interfaces are not user-configurable, and the information is for debugging purposes only.
prefix	(Optional) Prefix generated from a local IPv6 prefix pool. The prefix is the network portion of the IPv6 address.

Command Default

Displays all IPv6 interfaces.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show ipv6 interface** command provides output similar to the **show interface** command, except that it is IPv6-specific. If the interface hardware is usable, the interface is marked up. If the interface can provide two-way communication, the line protocol is marked up.

When an interface name is not specified, information on all IPv6 interfaces is displayed. Specifying an interface name displays information about the specified interface.

Examples

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

```
> show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

The following is sample output from the **show ipv6 interface** command when entered with the **brief** keyword:

```
> show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

The following is sample output from the **show ipv6 interface** command. It shows the characteristics of an interface which has generated a prefix from an address.

```
> show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 local pool

To display IPv6 address pool information, use the **show ipv6 local pool** command.

show ipv6 local pool *pool_name*

Syntax Description

pool_name	The name of an IPv6 address pool.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to view the contents of IPv6 address pools. These pools are used with remote access VPN and clustering. Use **show ip local pool** to view IPv4 address pools.

Examples

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

```
> show ipv6 local pool test-ipv6-pool
IPv6 Pool test-ipv6-pool
Begin Address: 2001:db8::db8:800:200c:417a
End Address: 2001:db8::db8:800:200c:4188
Prefix Length: 64
Pool Size: 15
Number of used addresses: 0
Number of available addresses: 15

Available Addresses:
2001:db8::db8:800:200c:417a
2001:db8::db8:800:200c:417b
2001:db8::db8:800:200c:417c
2001:db8::db8:800:200c:417d
2001:db8::db8:800:200c:417e
2001:db8::db8:800:200c:417f
2001:db8::db8:800:200c:4180
2001:db8::db8:800:200c:4181
2001:db8::db8:800:200c:4182
2001:db8::db8:800:200c:4183
2001:db8::db8:800:200c:4184
2001:db8::db8:800:200c:4185
2001:db8::db8:800:200c:4186
2001:db8::db8:800:200c:4187
2001:db8::db8:800:200c:4188
```

show ipv6 mld traffic

To display the Multicast Listener Discovery (MLD) traffic counter information, use the **show ipv6 mld traffic** command.

show ipv6 mld traffic

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show ipv6 mld traffic** command allows you to check if the expected number of MLD messages have been received and sent. The following information is provided by the **show ipv6 mld traffic** command:

- Elapsed time since counters cleared—The amount of time since the counters were cleared.
- Valid MLD Packets—The number of valid MLD packets that are received and sent.
- Queries—The number of valid queries that are received and sent.
- Reports—The number of valid reports that are received and sent.
- Leaves—The number of valid leaves received and sent.
- Mtrace packets—The number of multicast trace packets that are received and sent.
- Errors—The types of errors and the number of errors that have occurred.

Examples

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

```
> show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
                  Received          Sent
Valid MLD Packets  1                 3
Queries            1                 0
Reports            0                 3
Leaves             0                 0
Mtrace packets     0                 0
Errors:
Malformed Packets  0
Martian source     0
Non link-local source 0
Hop limit is not equal to 1 0
```

Related Commands

Command	Description
clear ipv6 mld traffic	Resets all MLD traffic counters.

show ipv6 neighbor

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbor** command.

show ipv6 neighbor [*if_name* | *address*]

Syntax Description

address	(Optional) Displays neighbor discovery cache information for the supplied IPv6 address only.
if_name	(Optional) Displays cache information for the supplied interface name. If you show all interfaces, then you also see information about internal interfaces that are used for system communications. Internal interfaces are not user-configurable, and the information is for debugging purposes only.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The following information is provided by the **show ipv6 neighbor** command:

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

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (Incomplete) and REACH (Reachable) states are different for dynamic and static cache entries.

The following are possible states for dynamic entries in the IPv6 neighbor discovery cache:

- INCMP—(Incomplete) Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.
- REACH—(Reachable) Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.
- STALE—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.
- DELAY—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last

DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.

- PROBE—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.
- ????—Unknown state.

The following are possible states for static entries in the IPv6 neighbor discovery cache:

- INCMP—(Incomplete) The interface for this entry is down.
- REACH—(Reachable) The interface for this entry is up.

- Interface

  The interface from which the address was reachable.

Examples

The following is sample output from the **show ipv6 neighbor** command when entered with an interface:

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

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

```
> show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                            Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e  REACH inside
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.

show ipv6 ospf

To display general information about OSPFv3 routing processes, use the **show ipv6 ospf** command.

show ipv6 ospf [*process_id*] [*area_id*]

Syntax Description

area_id	(Optional) Shows information about a specified area only.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPFv3 routing process is enabled.

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
```

Related Commands

Command	Description
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).
show ipv6 ospf database	Shows lists of information related to the OSPFv3 database for a specific router.

show ipv6 ospf border-routers

To display the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR), use the **show ipv6 ospf border-routers** command.

show ipv6 ospf [*process_id*] **border-routers**

Syntax Description

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPFv3 routing process is enabled.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show ipv6 ospf border-routers** command lists the following settings:

- Intra-area route
- Inter-area route
- IPv6 address
- Interface type
- Area ID
- SPF number

Examples

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

```
> show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf database	Shows lists of information related to the OSPFv3 database for a specific router.

show ipv6 ospf database

To display lists of information related to the OSPFv3 database for a specific router, use the **show ipv6 ospf database** command.

show ipv6 ospf [*process_id*] [*area_id*] **database** [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]

Syntax Description

adv-router *router-id*	(Optional) Displays all the LSAs of the advertising router. The router ID must be in the form documented in RFC 2740, in which the address is specified in hexadecimal using 16-bit values between colons.
area	(Optional) Displays information only about area LSAs.
area_id	(Optional) Displays information about a specified area only.
as	(Optional) Filters unknown autonomous system (AS) LSAs.
database-summary	(Optional) Displays how many of each type of LSA exists for each area in the database and the total.
destination-router-id	(Optional) Displays information about a specified destination router only.
external	(Optional) Displays information only about the external LSAs.
interface	Optional) Displays information about the LSAs filtered by interface context.
interface-name	(Optional) Specifies the LSA interface name.
internal	(Optional) Displays information only about the internal LSAs.
inter-area prefix	(Optional) Displays information only about LSAs based on inter-area prefix.
inter-area router	(Optional) Displays information only about LSAs based on inter-area router LSAs.
link	(Optional) Displays information about link LSAs. When it follows the **unknown** keyword, the **link** keyword filters link-scope LSAs.
link-state-id	(Optional) Specifies an integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
network	(Optional) Displays information about network LSAs.
nssa-external	(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.
prefix *ipv6-prefix*	(Optional) Displays the link-local IPv6 address of the neighbor. The IPv6 prefix must be in the form documented in RFC 2373, in which the address is specified in hexadecimal using 16-bit values between colons.

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
ref-lsa	(Optional) Further filters the prefix LSA type.
router	(Optional) Displays information about router LSAs.
self-originate	(Optional) Displays only self-originated LSAs from the local router.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The various forms of the command provide information about different OSPFv3 LSAs.

Examples

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

```
> show ipv6 ospf database

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

                Router Link States (Area 0)

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

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)

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

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

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

            Intra Area Prefix Link States (Area 0)

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

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf events

To display OSPFv3 internal event information, use the **show ipv6 ospf events** command.

show ipv6 ospf [*process_id*] **events** [*type*]

Syntax Description

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
type	(Optional) A list of the event types you want to see. If you do not specify one or more types, you see all events. You can filter on the following types: • **generic**—Generic events. • **interface**—Interface state change events. • **lsa**—LSA arrival and LSA generation events. • **neighbor**—Neighbor state change events. • **reverse**—Show events in reverse order. • **rib**—Router Information Base update, delete and redistribution events. • **spf**—SPF scheduling and SPF run events.

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 ospf events

OSPFv3 Router with ID (10.1.3.2) (Process ID 10)

   1 Jul 9  18:49:34.071: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
   2 Jul 9  18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2,

Seq# 80000008, Age 1, Area 10
   3 Jul 9  18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004,
Age    0, Area 10
   4 Jul 9  18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005,

Age 0, Area 10
   5 Jul 9  18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
   6 Jul 9  18:41:18.902: Starting External processing in area 10
   7 Jul 9  18:41:18.902: Starting External processing
   8 Jul 9  18:41:18.902: Starting Inter-Area SPF in area 10
   9 Jul 9  18:41:18.902: Generic:  post_spf_intra  0x0
  10 Jul 9  18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
```

```
  11 Jul 9  18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
  12 Jul 9  18:41:18.902: Starting Intra-Area SPF in Area 10
  13 Jul 9  18:41:18.903: Starting SPF, wait-interval 5000ms
  14 Jul 9  18:41:16.403: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
  15 Jul 9  18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0,
Adv-Rtr   50.100.168.192
  16 Jul 9  18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,
Seq# 80000003, Age 1, Area 10
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf flood-list

To display a list of OSPFv3 LSAs waiting to be flooded over an interface, use the **show ipv6 ospf flood-list** command.

show ipv6 ospf [*process_id*] [*area_id*] **flood-list** *interface-type interface-number*

Syntax Description

area_id	(Optional) Displays information about a specified area only.
interface-number	Specifies the interface number over which the LSAs are flooded.
interface-type	Specifies the interface type over which the LSAs are flooded.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPFv3 routing process is enabled.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to display OSPFv3 packet pacing information.

Examples

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

```
> show ipv6 ospf flood-list

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971

 Interface FastEthernet0/0, Queue length 0

 Interface ATM3/0, Queue length 0
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf graceful-restart

To display information about OSPFv3 graceful-restart, use the **show ipv6 ospf graceful-restart** command.

show ipv6 ospf graceful-restart

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 ospf graceful-restart
Routing Process "ospfv3 10"
  Graceful Restart enabled
    restart-interval limit: 240 sec
    Clustering is not configured in spanned etherchannel mode
  Graceful Restart helper support enabled
    Number of neighbors performing Graceful Restart is 0
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.

show ipv6 ospf interface

To display OSPFv3-related interface information, use the **show ipv6 ospf interface** command.

show ipv6 ospf [*process_id*] [*area_id*] **interface** [*type-number*] [**brief**]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
brief	(Optional) Displays brief overview information for OSPFv3 interfaces, states, addresses and masks, and areas on the router.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
type-number	(Optional) Specifies the interface type and number.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to display overview information for OSPFv3 interfaces, states, addresses and masks, and areas on the router.

Examples

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

```
> show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
```

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

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf request-list

To display a list of all LSAs that have been requested by a router, use the **show ipv6 ospf request-list** command.

show ipv6 ospf [*process_id*] [*area_id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
interface	(Optional) Specifies the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Specifies the list of all LSAs requested by the router on this interface from this neighbor.
neighbor	(Optional) Specifies the list of all LSAs requested by the router from this neighbor.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 ospf request-list

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

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

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
  2      0.0.0.3         192.168.255.3   0x800000A9  774    0x0058C0
  2      0.0.0.2         192.168.255.3   0x800000B7  1      0x003A63
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf retransmission-list

To display a list of all LSAs that have been waiting to be resent, use the **show ipv6 ospf retransmission-list** command.

show ipv6 ospf [*process_id*] [*area_id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
interface	(Optional) Specifies the list of all LSAs waiting to be resent on this interface.
interface-neighbor	(Optional) Specifies the list of all LSAs waiting to be resent for this interface from this neighbor.
neighbor	(Optional) Specifies the list of all LSAs waiting to be resent for this neighbor.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 ospf retransmission-list

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

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

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

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf statistic

To display various OSPFv3 statistics, such as the number of times SPF was executed, the reasons, and the duration, use the **show ipv6 ospf statistic** command.

show ipv6 ospf [*process_id*] **statistic** [**detail**]

Syntax Description

detail	(Optional) Specifies detailed SPF information, including the trigger points.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 ospf 10 statistic detail
Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0             0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
  50.100.168.192/2(N)
```

show ipv6 ospf summary-prefix

To display a list of all summary address redistribution information configured under an OSPFv3 process, use the **show ipv6 ospf summary-prefix** command.

show ipv6 ospf [*process_id*] **summary-prefix**

Syntax Description

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix

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

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf timers

To display OSPFv3 timers information, use the **show ipv6 ospf timers** command.

show ipv6 ospf [*process_id*] **timers** [**lsa-group** | **rate-limit**]

Syntax Description

lsa-group	(Optional) Specifies OSPFv3 LSA group information.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
rate-limit	(Optional) Specifies OSPFv3 LSA rate limit information.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show ipv6 ospf timers lsa-group** command:

```
> show ipv6 ospf timers lsa-group

OSPFv3 Router with ID (10.10.13.101) (Process ID 1)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:13
Current time 96532
Index 0 Timestamp 96546
Index 1 Timestamp 96788
Index 2 Timestamp 97048
Index 3 Timestamp 97293
Index 4 Timestamp 97548

Failure Head 0, Last 0 LSA group failure logged

            OSPFv3 Router with ID (10.10.10.102) (Process ID 5709)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:22
Current time 96532
Index 0 Timestamp 96555
Index 1 Timestamp 96801
Index 2 Timestamp 97041
Index 3 Timestamp 97287
Index 4 Timestamp 97546

Failure Head 0, Last 0 LSA group failure logged
```

show ipv6 ospf traffic

To display OSPFv3 traffic-related statistics for currently available interfaces, use the **show ipv6 ospf traffic** command.

show ipv6 ospf [*process_id*] **traffic** [*interface_name*]

Syntax Description

interface_name	(Optional) Specifies the name of the interface. Use this option to segregate traffic to a specific interface.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 ospf 10 traffic inside
Interface inside

Last clearing of interface traffic counters never

OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid                       0 0
  RX Hello                      1232 53132
  RX DB des                       27 896
  RX LS req                        3 216
  RX LS upd                       28 2436
  RX LS ack                       14 1064
  RX Total                      1304 57744

  TX Failed                        0 0
  TX Hello                       753 32072
  TX DB des                       27 1056
  TX LS req                        2 92
  TX LS upd                        9 1128
  TX LS ack                       15 900
  TX Total                       806 35248
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf virtual-links

To display parameters and the current state of OSPFv3 virtual links, use the **show ipv6 ospf virtual-links** command.

show ipv6 ospf virtual-links

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show ipv6 ospf virtual-links

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

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 prefix-list

To list prefix lists that are configured to match IPv6 traffic, use the **show ipv6 prefix-list** command.

show ipv6 prefix-list [**detail** | **summary**] [*prefix_list_name* [**seq** *sequence_number* | *network/length* [**longer** | **first-match**]]]

Syntax Description

detail	Show details about prefix lists.
summary	Show a summary of prefix lists.
prefix_list_name	Name of a prefix list.
seq *sequence_number*	(Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix list.
network/length [**longer** | **first-match**]	(Optional) Displays all entries in the specified prefix list that use this network address and prefix length (in bits). You can optionally include one of the following keywords: • **longer** displays all entries of the specified prefix list that match or are more specific than the given network/length. • **first-match** displays the first entry of the specified prefix list that matches the given network/length.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show ipv6 prefix-list** command.

```
> show ipv6 prefix-list
ipv6 prefix-list test-ipv6-prefix: 1 entries
   seq 5 permit 2001:db8:0:cd30::/64
```

The following is an example of summarized output.

```
> show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

The following is an example of detailed output.

```
> show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: test-ipv6-prefix
```

```
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

Related Commands

Command	Description
clear ipv6 prefix-list	Reset the hit count on an IPv6 prefix list.
show bgp prefix-list	Displays information about a prefix list or prefix list entries in the context of Border Gateway Protocol.
show prefix-list	Displays information about IPv4 prefix lists.

show ipv6 route

To display the contents of the IPv6 routing table, use the **show ipv6 route** command.

show ipv6 route [**vrf** *name* | **all**] [**management-only**] [**failover**] [**cluster**] [**interface** *name*] [**ospf**] [**summary**]

Syntax Description

managment-only	Displays routes in the IPv6 management routing table.
cluster	(Optional) Displays the IPv6 routing table sequence number, IPv6 reconvergence timer status, and IPv6 routing entries sequence number in a cluster.
failover	(Optional) Displays the IPv6 routing table sequence number, IPv6 reconvergence timer status, and IPv6 routing entries sequence number.
interface *name*	(Optional) Displays IPv6 interface-specific routes.
ospf	(Optional) Displays OSPFv3 routes.
summary	(Optional) Displays IPv6 route summaries.
[**vrf** *name* | **all**]	If you enable virtual routing and forwarding (VRF), also known as virtual routers, you can limit the view to a specific virtual router using the **vrf** *name* keyword. If you want to see the routing tables for all virtual routers, include the **all** keyword. If you include neither of these VRF-related keywords, the command shows the routing table for the global VRF virtual router.

Command History

Release	Modification
6.1	This command was introduced.
6.6	The [**vrf** *name* | **all**] keywords were added.

Usage Guidelines

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

The following information appears in the IPv6 routing table:

- Codes—Indicates the protocol that derived the route. Values are as follows:
  - C—Connected
  - L—Local
  - S—Static
  - R—RIP derived
  - B—BGP derived
  - I1—ISIS L1—Integrated IS-IS Level 1 derived
  - I2—ISIS L2—Integrated IS-IS Level 2 derived

    - IA—ISIS interarea—Integrated IS-IS interarea derived

- fe80::/10—Indicates the IPv6 prefix of the remote network.
- [0/0]—The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
- via ::—Specifies the address of the next router to the remote network.
- inside—Specifies the interface through which the next router to the specified network can be reached.

Examples

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

```
> show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

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

```
> show ipv6 route failover

IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
           ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired

O   2009::1/128 [110/10]
     via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
     via fe80::217:94ff:fe85:4401, inside seq 0
S   4001::1/128 [0/0]
     via 4001::2, inside seq 0
C   7001::1/128 [0/0]
     via ::, outside seq 0
L   fe80::/10 [0/0]
```

```
     via ::, inside seq 0
     via ::, outside seq 0
L    ff00::/8 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
```

The following is sample output from the s**how ipv6 route cluster** command on the primary unit:

```
> show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 2
IPv6 Reconvergence timer expired

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

The following is sample output from the **show ipv6 route cluster** command on the secondary unit during a role change:

```
> cluster master
INFO: Wait for existing master to quit. Use "show cluster info"
to check status. Use "cluster remove unit <name>" to force
master unit out of the cluster if for some reason it refuses
to quit within reasonable time
> show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 3
IPv6 Reconvergence timer expires in 61 secs

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

The following example displays routes for the virtual router named red. Note that static routes leaked to other virtual routers are indicated with the key SI.

```
> show ipv6 route vrf red

Codes: C - Connected, L - Local, S - Static, SI - Static InterVRF
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP, V - VPN
            I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

IPv6 Routing Table : red - 5 entries
L   2301::/128 [0/0]
     via ::, gig0
C   2301::/64 [0/0]
     via ::, gig0
SI  2304::/64 [1/0]
     via ::, gig3
L   fe80::/10 [0/0]
```

```
     via ::, gig0
L    ff00::/8 [0/0]
     via ::, gig0
```

Related Commands

Command	Description
show route	Displays the IPv4 routing table.
show vrf	Shows the virtual routers defined on the system.

show ipv6 routers

To display IPv6 router advertisement information received from on-link routers, use the **show ipv6 routers** command.

show ipv6 routers [*if_name*]

Syntax Description

if_name	(Optional) The internal or external interface name that you want to display information about.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

When an interface name is not specified, information on all IPv6 interfaces is displayed. Specifying an interface name displays information about the specified interface.

Examples

The following is sample output from the **show ipv6 routers** command when entered without an interface name:

```
> show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

Related Commands

Command	Description
ipv6 route	Adds a static entry to the IPv6 routing table.

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show ipv6 traffic** command.

show ipv6 traffic

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use the **clear ipv6 traffic** command to clear the traffic counters.

Examples

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

```
> show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

Related Commands

Command	Description
clear ipv6 traffic	Clears IPv6 traffic counters.

show isakmp sa

To display the IKE runtime SA database, use the **show isakmp sa** command.

show isakmp sa [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example displays detailed information about the SA database:

```
> show isakmp sa detail

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

Related Commands

Command	Description
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active ISAKMP configuration.

show isakmp stats

To display runtime statistics, use the **show isakmp stats** command.

Threat Defense

show isakmp stats

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Each one of the counters maps to an associated cikePhase1GW counter. For details on each of these counters, refer to CISCO-IPSEC-FLOW-MONITOR-MIB.my.

- Active/Standby Tunnels—cikePhase1GWActiveTunnels
- Previous Tunnels—cikePhase1GWPreviousTunnels
- In Octets—cikePhase1GWInOctets
- In Packets—cikePhase1GWInPkts
- In Drop Packets—cikePhase1GWInDropPkts
- In Notifys—cikePhase1GWInNotifys
- In P2 Exchanges—cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids—cikePhase1GWInP2ExchgInvalids
- In P2 Exchange Rejects—cikePhase1GWInP2ExchgRejects
- In P2 Sa Delete Requests—cikePhase1GWInP2SaDelRequests
- Out Octets—cikePhase1GWOutOctets
- Out Packets—cikePhase1GWOutPkts
- Out Drop Packets—cikePhase1GWOutDropPkts
- Out Notifys—cikePhase1GWOutNotifys
- Out P2 Exchanges—cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids—cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects—cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests—cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels—cikePhase1GWInitTunnels
- Initiator Fails—cikePhase1GWInitTunnelFails
- Responder Fails—cikePhase1GWRespTunnelFails
- System Capacity Fails—cikePhase1GWSysCapFails

- Auth Fails—cikePhase1GWAuthFails
- Decrypt Fails—cikePhase1GWDecryptFails
- Hash Valid Fails—cikePhase1GWHashValidFails
- No Sa Fails—cikePhase1GWNoSaFails

Examples

The following example displays ISAKMP statistics:

```
> show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
```

Related Commands

Command	Description
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active ISAKMP configuration.

show isis database

To display the IS-IS link-state database, use the **show isis database** command.

show isis database [{**detail** | **verbose**} [**ip** [**unicast**] | **ipv6** [**unicast**]] [**topology base**]] [**level-1** | **level-2**]

Syntax Description

level-1	(Optional) Displays the IS-IS link-state database for Level 1.
level-2	(Optional) Displays the IS-IS link-state database for Level 2.
ip	(Optional) Shows the IS-IS link-state database for the IPv4 address-family
ipv6	(Optional) Shows the IS-IS link-state database for the IPv6 address-family
detail	(Optional) Displays the contents of each link-state packet (LSP).
verbose	(Optional) Displays additional information about the Intermediate IS-IS database.
topology base	(Optional) Shows the MTR topology.
unicast	(Optional) Shows unicast address families.

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

The following table explains the output for this command.

Table 9: Fields in IS-IS Database Output

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

Field	Description
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP will stay in the LSDB before being completely removed.
ATT	The Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers will use the Attach bit to find the closest Level 2 router. They will point a default route to the closest Level 2 router.
P	The P bit. Detects if the intermediate systems is area partition repair-capable. Cisco and other vendors do not support area partition repair.
OL	The Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers will not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router will be sent to this router.
Area Address (Detail and Verbose output only.)	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
NLPID (Detail and Verbose output only.)	Network Layer Protocol identifier.
Hostname (Detail and Verbose output only.)	Hostname of the node.
Router ID (Detail and Verbose output only.)	Traffic engineering router identifier for the node.
IP Address (Detail and Verbose output only.)	IPv4 address for the interface.
Metric (Detail and Verbose output only.)	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system (ES), or a Connectionless Network Service [CLNS] prefix).
Affinity (Verbose output only.)	Link attribute flags that are being flooded.

Field	Description
Physical BW (Verbose output only.)	Link bandwidth capacity (in bits per second).
Reservable BW (Verbose output only.)	Amount of reservable bandwidth on this link.
BW Unreserved (Verbose output only.)	Amount of bandwidth that is available for reservation.

Examples

The following example shows the IS-IS database.

```
> show isis database

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d300     0x3d0d              674                0/0/0
routerA.00-00     0x1b541556     0xa349               928                0/0/0
c3.00-00              0x9257c979     0x9952              759                0/0/0
c2.00-00             *0xef11e977     0x3188              489                0/0/0
c2.01-00             *0xa8333f03     0xd6ea              829                0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f24      0xaba2              526                0/0/0
routerA.00-00     0x0d540b55      0x81d7              472                0/0/0
routerA.00-01     0xffffff01          0xe20b             677                0/0/0
c3.00-00              0x002e5434      0xb20a             487                0/0/0
c2.00-00             *0x74fd1227      0xbb0f             742                0/0/0
c2.01-00             *0x7ee72c1a      0xb506             968                0/0/0
```

The following example shows detailed output for the IS-IS database. Detailed output displays the contents of each LSP.

```
> show isis database detail

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d301      0x3b0e              1189               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00      0x1b541556     0xa349               642                0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
```

```
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

The following example shows detailed output for a Level 2 LSP only. The area address 39.0001 is the address of the area in which the router resides.

```
> show isis database l2 detail

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f25      0xa9a3              1076                     0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IS c2.01
routerA.00-00     0x0d540b56     0x7fd8                941                      0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IS c2.01
  Metric:          0 IP-External 1.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.2.2.0 255.255.255.0
  Metric:          0 IP-External 3.1.1.0 255.255.255.0
```

The following example shows verbose output.

```
> show isis database verbose

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00             *0xea19d301   0x3b0e        644               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   22.22.22.1
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00         0x1b541557   0xa14a        783               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   22.22.22.5
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

Related Commands

Command	Description
clear isis	Clears IS-IS data structures.
show clns	Shows CLNS-specific information.
show route isis	Shows IS-IS routes.

show isis hostname

To display the router-name-to-system-ID mapping table entries for an IS-IS router, use the **show isis hostname** command.

show isis hostname

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

In the IS-IS routing domain, the system ID is used to represent each router. The system ID is part of the network entity title (NET) that is configured for each IS-IS router. For example, a router with a configured NET of 49.0001.0023.0003.000a.00 has a system ID of 0023.0003.000a. Router-name-to-system-ID mapping is difficult for network administrators to remember during maintenance and troubleshooting on the routers. Entering the **show isis hostname** command displays the entries in the router-name-to-system-ID mapping table.

Examples

The following example displays the dynamic host mapping table. The dynamic host mapping table displays the router-name-to-system-ID mapping table entries for ciscothreat defense, c2, c3 and for the local router named routerA. The table also shows that c3 is a Level-1 router, and its hostname is advertised by the Level-1 (L1) link-state protocol (LSP). C2 is a Level-2 router and its hostname is advertised by the L2 LSP. The * symbol that appears under Level for ciscothreat defense signifies that this is the router-name-to-system-ID mapping information for the system.

```
> show isis hostname

Level  System ID       Dynamic Hostname  (c1)
     * 0050.0500.5005   ciscoASA
    1  0050.0500.5007   c3
    2  0050.0500.5006   routerA
    2  0050.0500.5008   c2
```

Related Commands

Command	Description
clear isis	Clears IS-IS data structures.
show clns	Shows CLNS-specific information.
show route isis	Shows IS-IS routes.

show isis lsp-log

To display the Level 1 and Level 2 IS-IS link-state packet (LSP) log of the interfaces that triggered the new LSP, use the **show isis lsp-log** command.

show isis lsp-log

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

Use this command to display the Level 1 and Level 2 IS-IS link-state packet (LSP) log of the interfaces that triggered the new LSP. The output includes the following information:

- When—The time elapsed since the LSP was generated.
- Count—The number of events that took place at this time.
- Interface—The interface that caused the LSP regeneration.
- Triggers—The event that triggered the LSP to be flooded. Possible triggers for an LSP are as follows:
  - AREASET—Active area set changed.
  - ATTACHFLAG—Attach bit changed state.
  - CLEAR—Some form of manual clear command was issued.
  - CONFIG—Any configuration change.
  - DELADJ—Adjacency went down.
  - DIS—DIS changed or pseudonode changed.
  - ES—End System adjacency changed.
  - HIPPITY—LSPDB overload bit changed state.
  - IF_DOWN—Needs a new LSP.
  - IP_DEF_ORIG—Default information originate changed.
  - IPDOWN—Directly connected IP prefix down.
  - IP_EXTERNAL—Redistributed IP route appeared or gone.
  - IPIA—Interarea IP route appeared or gone.
  - IPUP—Directly connected IP prefix up.
  - NEWADJ—New adjacency came up.
  - REDIST—Redistributed level-2 CLNS route changed.
  - RRR_INFO—RRR bandwidth resource information.

Examples

The following is sample output from the **show isis lsp-log** command:

```
> show isis lsp-log

  Level 1 LSP log
When       Count       Interface         Triggers
04:16:47     1         subint             CONFIG NEWADJ DIS
03:52:42     2         subint             NEWADJ DIS
03:52:12     1         subint             ATTACHFLAG
03:31:41     1         subint             IPUP
03:30:08     2         subint             CONFIG
03:29:38     1         subint             DELADJ
03:09:07     1         subint             DIS ES
02:34:37     2         subint             NEWADJ
02:34:07     1         subint             NEWADJ DIS

  Level 2 LSP log
When       Count       Interface         Triggers
03:09:27     1         subint             CONFIG NEWADJ
03:09:22     1         subint             NEWADJ
02:34:57     2         subint             DIS
02:34:50     1                                IPUP
02:34:27     1         subint             CONFIG DELADJ
02:13:57     1         subint             DELADJ
02:13:52     1         subint             NEWADJ
01:35:58     2         subint             IPIA
01:35:51     1                              AREASET IPIA
```

Related Commands

Command	Description
clear isis	Clears IS-IS data structures.
show clns	Shows CLNS-specific information.
show route isis	Shows IS-IS routes.

show isis neighbors

To display information about IS-IS neighbors, use the **show isis neighbors** command.

show isis neighbors [**detail**]

Syntax Description

detail	(Optional) Displays more detailed information for IS-IS neighbors.

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

The following table explains the IS-IS neighbor information.

Table 10: IS-IS Neighbor Information

Field	Description
System Id	Six-byte value that identifies a system in an area.
Type	Level type. Indicates whether the IS-IS neighbor is a Level 1, Level-1-2, or Level 2 router.
Interface	Interface from which the system was learned.
IP Address	IP address of the neighbor router.
State	Indicates whether the state of the IS-IS neighbor is up or down.
Holdtime	Link-state packet (LSP) holdtime. Amount of time that the LSP remains valid (in seconds).
Circuit Id	Port location for the IS-IS neighbor router that indicates how it is connected to the local router.
Area Address(es)	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
SNPA	Subnetwork point of attachment. This is the data-link address.
State Changed	The time of the state change.
LAN Priority	Priority of the LAN.
Remote TID	Neighbor router topology IDs.
Local TID	Local router topology IDs.

Examples

The following example shows basic IS-IS neighbor information.

```
> show isis neighbors

System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint   10.22.22.5        UP    21          c2.01
routerA          L2    subint   10.22.22.5        UP    22          c2.01
c2               L1    subint   10.22.22.3        UP     9          c2.01
c2               L2    subint   10.22.22.3        UP     9          c2.01
```

The following example shows detailed IS-IS neighbor information.

```
> show isis neighbors detail

System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint   10.22.22.5        UP    23          c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
routerA          L2    subint   10.22.22.5        UP    22         c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
```

Related Commands

Command	Description
clear isis	Clears IS-IS data structures.
show clns	Shows CLNS-specific information.
show route isis	Shows IS-IS routes.

show isis rib

To display paths for a specific route or for all routes under a major network that are stored in the IP local Routing Information Base (RIB), use the **show isis rib** command.

show isis [***** | **ip** [**unicast**] | **ipv6** [**unicast**]] **rib** [**redistribution** [**level-1** | **level-2**]] [*network_ip* [*mask*]]

Syntax Description

*****	(Optional) Shows all IS-IS address families.
ip	(Optional) Shows the IPv4 address family.
ipv6	(Optional) Shows the IPv6 address family.
level-1	(Optional) Shows the Level 1 redistribution RIB.
level-2	(Optional) Shows the Level 2 redistribution RIB
network_ip [*mask*]	(Optional) Shows RIB information for a network.
redistribution	(Optional) Shows IS-IS IP redistribution RIB information
unicast	(Optional) Shows the unicast address family.

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

Use this command to verify that an IP prefix update that exists in the IP global RIB also has been updated in the IS-IS local RIB.

Examples

The following is example shows all routes that are stored within the IS-IS local RIB.

```
> show isis rib

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =

10.10.0.0 255.255.0.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

The following example shows all routes under the major network 10.0.0.0 with the IP address 10.3.2.0 that are stored within the IS-IS local RIB.

```
> show isis rib 10.3.2.0

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = =
Routes under majornet 10.0.0.0 255.0.0.0:

10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

The following example shows all routes under the network with the IP address and mask 10.3.2.0 255.255.255.0 that are stored within the IS-IS local RIB.

```
> show isis rib 10.3.2.0 255.255.255.0

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = =

10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

Related Commands

Command	Description
clear isis	Clears IS-IS data structures.
show clns	Shows CLNS-specific information.
show route isis	Shows IS-IS routes.

show isis spf-log

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

show isis [***** | **ip** [**unicast**] | **ipv6** [**unicast**]] **spf-log**

Syntax Description

*****	(Optional) Shows all IS-IS address families.
ip	(Optional) Shows the IPv4 address family.
ipv6	(Optional) Shows the IPv6 address family.
unicast	(Optional) Shows the unicast address family.

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

This command displays how often and why the router has run a full shortest path first (SPF) calculation. The following table explains the fields in the output.

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

The following table explains the possible triggers.

Trigger	Description
ATTACHFLAG	This router is now attached to the Level 2 backbone or it has just lost contact to the Level 2 backbone.
ADMINDIST	Another administrative distance was configured for the IS-IS process on this router.
AREASET	Set of learned area addresses in this area changed.
BACKUPOVFL	An IP prefix disappeared. The router knows there is another way to reach that prefix but has not stored that backup route. The only way to find the alternative route is through a full SPF run.
DBCHANGED	A **clear isis *** command was issued on this router.
IPBACKUP	An IP route disappeared, which was not learned via IS-IS, but via another protocol with better administrative distance. IS-IS will run a full SPF to install an IS-IS route for the disappeared IP prefix.
IPQUERY	A **clear ip route** command was issued on this router.
LSPEXPIRED	Some LSP in the link-state database (LSDB) has expired.
LSPHEADER	ATT/P/OL bits or is-type in an LSP header changed.
NEWADJ	This router has created a new adjacency to another router.
NEWAREA	A new area (via network entity title [NET]) was configured on this router.
NEWLEVEL	A new level (via is-type) was configured on this router.
NEWLSP	A new router or pseudonode appeared in the topology.
NEWMETRIC	A new metric was configured on an interface of this router.
NEWSYSID	A new system ID (via NET) was configured on this router.
PERIODIC	Typically, every 15 minutes a router runs a periodic full SPF calculation.
RTCLEARED	A **clear clns route** command was issued on this router.
TLVCODE	TLV code mismatch, indicating that different TLVs are included in the newest version of an LSP.
TLVCONTENT	TLV contents changed. This normally indicates that an adjacency somewhere in the area has come up or gone down. The "First trigger LSP" column indicates where the instability may have occurred.

Examples

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

```
> show isis ipv6 spf-log
```

```
      TID 0 level 1 SPF log
  When   Duration  Nodes  Count     First trigger LSP   Triggers
00:15:46    3124     40      1          milles.00-00  TLVCODE
00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP
00:15:19    3096     41      1          deurze.00-00  TLVCODE
00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER
00:14:49    3384     41      1          milles.00-01  TLVCODE
00:14:23    2932     41      3          milles.00-00  TLVCODE
00:05:18    3140     41      1                        PERIODIC
00:03:54    3144     41      1          milles.01-00  TLVCODE
00:03:49    2908     41      1          milles.01-00  TLVCODE
00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT
00:03:15    3054     41      1          milles.00-00  TLVCODE
00:02:53    2958     41      1          mortel.00-00  TLVCODE
00:02:48    3632     41      2          milles.00-00  NEWADJ TLVCODE
00:02:23    2988     41      1          milles.00-01  TLVCODE
00:02:18    3016     41      1          gemert.00-00  TLVCODE
00:02:14    2932     41      1           bakel.00-00  TLVCONTENT
00:02:09    2988     41      2           bakel.00-00  TLVCONTENT
00:01:54    3228     41      1          milles.00-00  TLVCODE
00:01:38    3120     41      3            rips.03-00  TLVCONTENT
```

Related Commands

Command	Description
clear isis	Clears IS-IS data structures.
show clns	Shows CLNS-specific information.
show route isis	Shows IS-IS routes.

show isis topology

To display a list of all connected routers in all areas, use the **show isis topology** command.

show isis [***** | **ip** [**unicast**] | **ipv6** [**unicast**]] **topology** [**level-1** | **level-2**]

Syntax Description

*****	(Optional) Shows all IS-IS address families.
ip	(Optional) Shows the IPv4 address family.
ipv6	(Optional) Shows the IPv6 address family.
level-1	(Optional) Shows the Level 1 redistribution RIB.
level-2	(Optional) Shows the Level 2 redistribution RIB
unicast	(Optional) Shows the unicast address family.

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

Use the **show isis topology** command to verify the presence and connectivity between all routers in all areas. The fields are explained in the following table.

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

Examples

The following example shows output from the **show isis topology** command.

```
> show isis topology

IS-IS TID 0 paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                  --
routerA                 10       routerA                 subint  0025.8407.f2b0
c3                      10
```

```
c2                      10           c2                subint  c08c.60e6.986f

IS-IS TID 0 paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                  --
routerA                 10       routerA                subint  0025.8407.f2b0
c3                      10
c2                      10           c2                subint  c08c.60e6.986f
```

Related Commands

Command	Description
clear isis	Clears IS-IS data structures.
show clns	Shows CLNS-specific information.
show route isis	Shows IS-IS routes.