CHAPTER 26

# show debug through show ipv6 traffic Commands

# show debug

To show the current debugging configuration in privileged EXEC mode, use the **show debug** command.

**show debug** [*command* [*keywords*]]

## Syntax Description

| | |
|---|---|
| *command* [*keywords*] | (Optional) Specifies the debug command whose current configuration you want to view. For each *command*, the syntax following *command* is identical to the syntax supported by the associated **debug** command. For example, valid *keywords* following **show debug aaa** are the same as the valid keywords for the **debug aaa** command. Thus, **show debug aaa** supports an **accounting** keyword, which lets you specify that you want to see the debugging configuration for that portion of AAA debugging. |

## Defaults

This command has no default settings.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Privileged EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Usage Guidelines

The valid *command* values follow. For information about valid syntax after *command*, see the entry for **debug** *command*, as applicable.

**Note** The availability of each *command* value depends upon the command modes that support the applicable **debug** command.

- **aaa**
- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**

- **ctm**
- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **email**
- **entity**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**

- **rtsp**
- **sdi**
- **sequence**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **xdmcp**

## Examples

The following commands enable debugging for authentication, accounting, and Flash memory. The **show debug** command is used in three ways to demonstrate how you can use it to view all debugging configuration, debugging configuration for a specific feature, and even debugging configuration for a subset of a feature.

```
hostname# debug aaa authentication
debug aaa authentication enabled at level 1
hostname# debug aaa accounting
debug aaa accounting enabled at level 1
hostname# debug disk filesystem
debug disk filesystem enabled at level 1
hostname# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
hostname# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
hostname# show debug aaa accounting
debug aaa accounting enabled at level 1
hostname#
```

## Related Commands

| Command | Description |
|---|---|
| **debug** | See all **debug** commands. |

# show dhcpd

To view DHCP binding, state, and statistical information, use the **show dhcpd** command in privileged EXEC or global configuration mode.

**show dhcpd** {**binding** [*IP_address*] | **state** | **statistics**}

## Syntax Description

| | |
|---|---|
| **binding** | Displays binding information for a given server IP address and its associated client hardware address and lease length. |
| *IP_address* | Shows the binding information for the specified IP address. |
| **state** | Displays the state of the DHCP server, such as whether it is enabled in the current context and whether it is enabled on each of the interfaces. |
| **statistics** | Displays statistical information, such as the number of address pools, bindings, expired bindings, malformed messages, sent messages, and received messages. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC or global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Usage Guidelines

If you include the optional IP address in the **show dhcpd binding** command, only the binding for that IP address is shown.

The **show dhcpd binding | state | statistics** commands are also available in global configuration mode.

## Examples

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

```
hostname# show dhcpd binding
IP Address Hardware Address Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

The following is sample output from the **show dhcpd state** command:

```
hostname# show dhcpd state
```

```
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
```

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

```
hostname# show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure dhcpd** | Removes all DHCP server settings. |
| **clear dhcpd** | Clears the DHCP server bindings and statistic counters. |
| **dhcpd lease** | Defines the lease length for DHCP information granted to clients. |
| **show running-config dhcpd** | Displays the current DHCP server configuration. |

# show dhcprelay state

To view the state of the DHCP relay agent, use the **show dhcprelay state** command in privileged EXEC or global configuration mode.

**show dhcprelay state**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC or global configuration | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 2.2(1) | This command was introduced. |
| 3.1(1) | This command was changed from **show dhcprelay**. |

## Usage Guidelines

This command displays the DHCP relay agent state information for the current context and each interface.

## Examples

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

```
hostname# show dhcprelay state

Context Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

## Related Commands

| Command | Description |
|---|---|
| **show dhcpd** | Displays DHCP server statistics and state information. |

| Command | Description |
|---|---|
| **show dhcprelay statistics** | Displays the DHCP relay statistics. |
| **show running-config dhcprelay** | Displays the current DHCP relay agent configuration. |

# show dhcprelay statistics

To display the DHCP relay statistics, use the **show dhcprelay statistics** command in privileged EXEC mode.

**show dhcprelay statistics**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 2.2(1) | This command was introduced. |
| 3.1(1) | This command was changed from **show dhcprelay**. |

## Usage Guidelines

The output of the **show dhcprelay statistics** command increments until you enter the **clear dhcprelay statistics** command.

## Examples

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

```
hostname# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
FeralPix(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure dhcprelay** | Removes all DHCP relay agent settings. |
| **clear dhcprelay statistics** | Clears the DHCP relay agent statistic counters. |
| **debug dhcprelay** | Displays debug information for the DHCP relay agent. |
| **show dhcprelay state** | Displays the state of the DHCP relay agent. |
| **show running-config dhcprelay** | Displays the current DHCP relay agent configuration. |

# show disk

To display the contents of the Flash memory, use the **show disk** command in privileged EXEC mode.

**show disk** [**filesys** | **all**]

## Syntax Description

| | |
|---|---|
| **filesys** | Shows information about the compact Flash card. |
| **all** | Shows the contents of Flash memory plus the file system information, |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | — | • |

## Command History

| Release | Modification |
|---|---|
| 2.2(1) | This command was introduced. |

## Examples

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

```
hostname# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 08:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

The following is sample output from the **show disk filesys** command:

```
hostname# show disk filesys
******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:           4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

## Related Commands

| Command | Description |
|---|---|
| **dir** | Displays the directory contents. |

# show dns-hosts

To show the DNS cache, use the **show dns-hosts** command in privileged EXEC mode.The DNS cache includes dynamically learned entries from a DNS server as well as manually entered name and IP addresses using the **name** command.

**show dns-hosts**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

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

## Examples

The following is sample output from the **show dns-hosts** command:

```
hostname# show dns-hosts
Host                        Flags      Age Type   Address(es)
ns2.example.com             (temp, OK) 0    IP    10.102.255.44
ns1.example.com             (temp, OK) 0    IP    192.168.241.185
snowmass.example.com        (temp, OK) 0    IP    10.94.146.101
server.example.com          (temp, OK) 0    IP    10.94.146.80
```

The **show dns-hosts** field descriptions are as follows:

| Field | Description |
|---|---|
| Host | Shows the hostname. |
| Flags | Shows the entry status, as a combination of the following:<br>• temp—This entry is temporary because it comes from a DNS server. The FWSM removes this entry after 72 hours of inactivity.<br>• perm—This entry is permanent because it was added with the **name** command.<br>• OK—This entry is valid.<br>• ??—This entry is suspect and needs to be revalidated.<br>• EX—This entry is expired. |
| Age | Shows the number of hours since this entry was last referenced. |
| Type | Shows the type of DNS record; this value is always IP. |
| Address(es) | The IP addresses. |

## Related Commands

| Command | Description |
|---|---|
| **clear dns-hosts cache** | Clears the DNS cache. |
| **dns domain-lookup** | Enables the FWSM to perform a name lookup. |
| **dns name-server** | Configures a DNS server address. |
| **dns retries** | Specifies the number of times to retry the list of DNS servers when the FWSM does not receive a response. |
| **dns timeout** | Specifies the amount of time to wait before trying the next DNS server. |

# show eigrp events

To display the EIGRP event log, use the **show eigrp events** command in privileged EXEC mode.

**show eigrp** [*as-number*] **events** [{*start end*} | **type**]

## Syntax Description

| | |
|---|---|
| *as-number* | (Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number. |
| *end* | (Optional) Limits the output to the entries with starting with the *start* index number and ending with the *end* index number. |
| *start* | (Optional) A number specifying the log entry index number. Specifying a start number causes the output to start with the specified event and end with the event specified by the *end* argument. Valid values are from 1 to 4294967295. |
| **type** | (Optional) Displays the events that are being logged. |

## Defaults

If a *start* and *end* is not specified, all log entries are shown.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Privileged EXEC | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 4.0(1) | This command was introduced. |

## Usage Guidelines

The **show eigrp events** output displays up to 500 events. Once the maximum number of events has been reached, new events are added to the bottom of the output and old events are removed from the top of the output.

You can use the **clear eigrp events** command to clear the EIGRP event log.

The **show eigrp events type** command displays the logging status of EIGRP events. By default, neighbor changes, neighbor warning, and DUAL FSM messages are logged. You can disable neighbor change event logging using the **no eigrp log-neighbor-changes** command. You can disable neighbor warning event logging using the **no eigrp log-neighbor-warnings** command. You cannot disable the logging of DUAL FSM events.

## Examples

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

```
hostname# show eigrp events

Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

The following is sample output from the **show eigrp events** command with a start and stop number defined:

```
hostname# show eigrp events 3 8

Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

The following is sample output from the **show eigrp events** command when there are no entries in the EIGRP event log:

```
hostname# show eigrp events

Event information for AS 100:  Event log is empty.
```

The following is sample output from the **show eigrp events type** command:

```
hostname# show eigrp events type

EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

## Related Commands

| Command | Description |
|---|---|
| **clear eigrp events** | Clears the EIGRP event logging buffer. |
| **eigrp log-neighbor-changes** | Enables the logging of neighbor change events. |
| **eigrp log-neighbor-warnings** | Enables the logging of neighbor warning events. |

# show eigrp interfaces

To display the interfaces participating in EIGRP routing, use the **show eigrp interfaces** command in privileged EXEC mode.

**show eigrp** [*as-number*] **interfaces** [*if-name*] [**detail**]

## Syntax Description

| | |
|---|---|
| *as-number* | (Optional) Specifies the autonomous system number of the EIGRP process for which you are displaying active interfaces. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number. |
| **detail** | (Optional) Displays detail information. |
| *if-name* | (Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name limits the display to the specified interface. |

## Defaults

If you do not specify an interface name, information for all EIGRP interfaces is displayed.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 4.0(1) | This command was introduced. |

## Usage Guidelines

Use the **show eigrp interfaces** command to determine on which interfaces EIGRP is active, and to learn information about EIGRP relating to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

## Examples

The following is sample output from the **show eigrp interfaces** command:

```
hostname# show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface    Peers  Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
```

```
mgmt            0          0/0          0       11/434          0          0
outside         1          0/0        337        0/10           0          0
inside          1          0/0         10        1/63         103          0
```

Table 26-1 describes the significant fields shown in the display.

*Table 26-1 show eigrp interfaces Field Descriptions*

| Field | Description |
|---|---|
| process | Autonomous system number for the EIGRP routing process. |
| Peers | Number of directly-connected peers. |
| Xmit Queue Un/Reliable | Number of packets remaining in the Unreliable and Reliable transmit queues. |
| Mean SRTT | Mean smooth round-trip time interval (in seconds). |
| Pacing Time Un/Reliable | Pacing time (in seconds) used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets). |
| Multicast Flow Timer | Maximum number of seconds in which the FWSM will send multicast EIGRP packets. |
| Pending Routes | Number of routes in the packets in the transmit queue waiting to be sent. |

## Related Commands

| Command | Description |
|---|---|
| **network** | Defines the networks and interfaces that participate in the EIGRP routing process. |

# show eigrp neighbors

To display the EIGRP neighbor table, use the **show eigrp neighbors** command in privileged EXEC mode.

**show eigrp** [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]

## Syntax Description

| | |
|---|---|
| *as-number* | (Optional) Specifies the autonomous system number of the EIGRP process for which you are deleting neighbor entries. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number. |
| **detail** | (Optional) Displays detail neighbor information. |
| *if-name* | (Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name displays all neighbor table entries that were learned through that interface. |
| **static** | (Optional) Displays EIGRP neighbors that are statically defined using the **neighbor** command. |

## Defaults

If you do not specify an interface name, the neighbors learned through all interfaces are displayed.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 4.0(1) | This command was introduced. |

## Usage Guidelines

You can use the **clear eigrp neighbors** command to clear the dynamically-learned neighbors from the EIGRP neighbor table.

Static neighbors are not included in the output unless you use the **static** keyword.

## Examples

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

```
hostname# show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100
Address                Interface  Holdtime Uptime   Q      Seq  SRTT  RTO
                                  (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28           Vlan10      13       0:00:41  0      11   4     20
```

```
172.16.80.28           Vlan10     14        0:02:01  0       10    12     24
172.16.80.31           Vlan10     12        0:02:02  0       4     5      20
```

Table 26-1 describes the significant fields shown in the display.

*Table 26-2 show eigrp neighbors Field Descriptions*

| Field | Description |
|---|---|
| process | Autonomous system number for the EIGRP routing process. |
| Address | IP address of the EIGRP neighbor. |
| Interface | Interface on which the FWSM receives hello packets from the neighbor. |
| Holdtime | Length of time (in seconds) that the FWSM waits to hear from the neighbor before declaring it down. This hold time is received from the neighbor in the hello packet, and begins decreasing until another hello packet is received from the neighbor.<br>If the neighbor is using the default hold time, this number will be less than 15. If the peer configures a non-default hold time, the non-default hold time will be displayed.<br>If this value reaches 0, the FWSM considers the neighbor unreachable. |
| Uptime | Elapsed time (in hours:minutes: seconds) since the FWSM first heard from this neighbor. |
| Q Count | Number of EIGRP packets (update, query, and reply) that the FWSM is waiting to send. |
| Seq Num | Sequence number of the last update, query, or reply packet that was received from the neighbor. |
| SRTT | Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the FWSM to receive an acknowledgment of that packet. |
| RTO | Retransmission timeout (in milliseconds). This is the amount of time the FWSM waits before resending a packet from the retransmission queue to a neighbor. |

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

```
hostname# show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
Static Address                 Interface
192.168.1.5                    management
```

Table 26-3 describes the significant fields shown in the display.

*Table 26-3 show ip eigrp neighbors static Field Descriptions*

| Field | Description |
|---|---|
| process | Autonomous system number for the EIGRP routing process. |
| Static Address | IP address of the EIGRP neighbor. |
| Interface | Interface on which the FWSM receives hello packets from the neighbor. |

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

```
hostname# show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5              Vlan10 11 00:04:07  768  4608  0  4    S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10             Vlan10 13 1w0d         1  3000  0  6    S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6              Vlan10 12 1w0d         1  3000  0  4    S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

Table 26-4 describes the significant fields shown in the display.

*Table 26-4 show ip eigrp neighbors details Field Descriptions*

| Field | Description |
|---|---|
| process | Autonomous system number for the EIGRP routing process. |
| H | This column lists the order in which a peering session was established with the specified neighbor. The order is specified with sequential numbering starting with 0. |
| Address | IP address of the EIGRP neighbor. |
| Interface | Interface on which the FWSM receives hello packets from the neighbor. |
| Holdtime | Length of time (in seconds) that the FWSM waits to hear from the neighbor before declaring it down. This hold time is received from the neighbor in the hello packet, and begins decreasing until another hello packet is received from the neighbor.<br>If the neighbor is using the default hold time, this number will be less than 15. If the peer configures a non-default hold time, the non-default hold time will be displayed.<br>If this value reaches 0, the FWSM considers the neighbor unreachable. |
| Uptime | Elapsed time (in hours:minutes: seconds) since the FWSM first heard from this neighbor. |
| SRTT | Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the FWSM to receive an acknowledgment of that packet. |
| RTO | Retransmission timeout (in milliseconds). This is the amount of time the FWSM waits before resending a packet from the retransmission queue to a neighbor. |
| Q Count | Number of EIGRP packets (update, query, and reply) that the FWSM is waiting to send. |
| Seq Num | Sequence number of the last update, query, or reply packet that was received from the neighbor. |
| Version | The software version that the specified peer is running. |
| Retrans | The number of times that a packet has been retransmitted. |

*Table 26-4 show ip eigrp neighbors details Field Descriptions*

| Field | Description |
|---|---|
| Retries | The number of times an attempt was made to retransmit a packet. |
| Restart time | Elapsed time (in hours:minutes: seconds) since the specified neighbor has restarted. |

## Related Commands

| Command | Description |
|---|---|
| **clear eigrp neighbors** | Clear the EIGRP neighbor table. |
| **debug eigrp neighbors** | Display EIGRP neighbor debug messages. |
| **debug ip eigrp** | Display EIGRP packet debug messages. |

# show eigrp topology

To display the EIGRP topology table, use the **show eigrp topology** command in privileged EXEC mode.

**show eigrp** [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

## Syntax Description

| | |
|---|---|
| **active** | (Optional) Displays only active entries in the EIGRP topology table. |
| **all-links** | (Optional) Displays all routes in the EIGRP topology table, even those that are not feasible successors. |
| *as-number* | (Optional) Specifies the autonomous system number of the EIGRP process. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number. |
| *ip-addr* | (Optional) The IP address from the topology table to display. When specified with a mask, a detailed description of the entry is provided. |
| *mask* | (Optional) The network mask to apply to the *ip-addr* argument. |
| **pending** | (Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor. |
| **summary** | (Optional) Displays a summary of the EIGRP topology table. |
| **zero-successors** | (Optional) Displays available routes in the EIGRP topology table. |

## Defaults

Only routes that are feasible successors are displayed. Use the **all-links** keyword to display all routes, including those that are not feasible successors.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 4.0(1) | This command was introduced. |

## Usage Guidelines

You can use the **clear eigrp topology** command to remove the dynamic entries from the topology table.

## Examples

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

```
hostname# show eigrp topology

EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.16.90.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Vlan10
          via 10.16.81.28 (46251776/46226176), Vlan10
P 10.16.81.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Vlan1
          via 10.16.81.28 (307200/281600), Vlan10
          via 10.16.80.28 (307200/281600), Vlan10
```

Table 26-5 describes the significant fields shown in the displays.

*Table 26-5 show eigrp topology Field Information*

| Field | Description |
|---|---|
| Codes | State of this topology table entry. Passive and Active refer to the EIGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent. |
| P - Passive | The route is known to be good and no EIGRP computations are being performed for this destination. |
| A - Active | EIGRP computations are being performed for this destination. |
| U - Update | Indicates that an update packet was sent to this destination. |
| Q - Query | Indicates that a query packet was sent to this destination. |
| R - Reply | Indicates that a reply packet was sent to this destination. |
| r - Reply status | Flag that is set after the software has sent a query and is waiting for a reply. |
| *address mask* | Destination IP address and mask. |
| successors | Number of successors. This number corresponds to the number of next hops in the IP routing table. If "successors" is capitalized, then the route or next hop is in a transition state. |
| FD | Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route went active. This value is used in the feasibility condition check. If the reported distance of the router (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the software determines it has a feasible successor, it need not send a query for that destination. |
| via | IP address of the peer that told the software about this destination. The first *n* of these entries, where *n* is the number of successors, is the current successors. The remaining entries on the list are feasible successors. |
| (*cost/adv_cost*) | The first number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised. |
| *interface* | The interface from which the information was learned. |

The following is sample output from the **show eigrp topology** used with an IP address. The output shown is for an internal route.

```
hostname# show eigrp topology 10.2.1.0 255.255.255.0

EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0
```

```
    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
        0.0.0.0 (Vlan10), from Connected, Send flag is 0x0
            Composite metric is (281600/0), Route is Internal
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 1000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 0
```

The following is sample output from the **show eigrp topology** used with an IP address. The output shown is for an external route.

```
hostname# show eigrp topology 10.4.80.0 255.255.255.0


EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
    Routing Descriptor Blocks:
        10.2.1.1 (Vlan10), from 10.2.1.1, Send flag is 0x0
            Composite metric is (409600/128256), Route is External
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 6000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 1
            External data:
                Originating router is 10.89.245.1
                AS number of route is 0
                External protocol is Connected, external metric is 0
                Administrator tag is 0 (0x00000000)
```

## Related Commands

| Command | Description |
|---|---|
| **clear eigrp topology** | Clears the dynamically discovered entries from the EIGRP topology table. |

# show eigrp traffic

To display the number of EIGRP packets sent and received, use the **show eigrp traffic** command in privileged EXEC mode.

**show eigrp** [*as-number*] **traffic**

## Syntax Description

| | |
|---|---|
| *as-number* | (Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number. |

## Defaults

No default behaviors or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | **Firewall Mode** | | **Security Context** | | |
|---|---|---|---|---|---|
| | | | | **Multiple** | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Privileged EXEC | • | — | • | — | — |

## Command History

| **Release** | **Modification** |
|---|---|
| 4.0(1) | This command was introduced. |

## Usage Guidelines

You can use the **clear eigrp traffic** command to clear the EIGRP traffic statistics.

## Examples

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

```
hostname# show eigrp traffic

EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

Table 26-3 describes the significant fields shown in the display.

*Table 26-6 show eigrp traffic Field Descriptions*

| Field | Description |
|---|---|
| process | Autonomous system number for the EIGRP routing process. |
| Hellos sent/received | Number of hello packets sent and received. |
| Updates sent/received | Number of update packets sent and received. |
| Queries sent/received | Number of query packets sent and received. |
| Replies sent/received | Number of reply packets sent and received. |
| Acks sent/received | Number of acknowledgment packets sent and received. |
| Input queue high water mark/drops | Number of received packets that are approaching the maximum receive threshold and number of dropped packets. |
| SIA-Queries sent/received | Stuck in active queries sent and received. |
| SIA-Replies sent/received | Stuck in active replies sent and received. |

## Related Commands

| Command | Description |
|---|---|
| **debug eigrp packets** | Displays debug information for EIGRP packets sent and received. |
| **debug eigrp transmit** | Displays debug information for EIGRP messages sent. |

# show failover

To display information about the failover status of the unit, use the **show failover** command in privileged EXEC mode.

**show failover** [**group** *num* | **history** | **interface** | **state** | **statistics**]

## Syntax Description

| | |
|---|---|
| **group** | Displays the running state of the specified failover group. |
| **history** | Displays failover history. The failover history displays past failover state changes and the reason for the state change. |
| **interface** | Displays failover command and stateful link information. |
| *num* | Failover group number. |
| **state** | Displays the failover state of both failover units. The information displayed includes the primary or secondary status of the unit, the Active/Standby status of the unit, and, if a unit is in the failed state, the reason for the failure. |
| **statistics** | Displays transmit and receive packet count of failover command interface. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |
| 2.1(1) | Support for the Autostate feature and suspend configuration synchronization were added. |
| 3.1(1) | This command was modified to include failover groups. The output includes additional information. |

## Usage Guidelines

The **show failover** command displays the dynamic failover information, interface status, and Stateful Failover statistics. The Stateful Failover Logical Update Statistics output appears only when Stateful Failover is enabled. The “xerr” and “rerr” values do not indicate errors in failover, but rather the number of packet transmit or receive errors.

In the **show failover** command output, the fields have the following values:

- Stateful Obj has these values:
  - xmit—Indicates the number of packets transmitted.

  - xerr—Indicates the number of transmit errors.
  - rcv—Indicates the number of packets received.
  - rerr—Indicates the number of receive errors.
- Each row is for a particular object static count as follows:
  - General—Indicates the sum of all stateful objects.
  - sys cmd—Refers to the logical update system commands, such as **login** or **stay alive**.
  - up time—Indicates the value for the FWSM up time, which the active FWSM passes on to the standby FWSM.
  - RPC services—Remote Procedure Call connection information.
  - TCP conn—Dynamic TCP connection information.
  - UDP conn—Dynamic UDP connection information.
  - ARP tbl—Dynamic ARP table information.
  - Xlate_Timeout—Indicates connection translation timeout information.
  - VPN IKE upd—IKE connection information.
  - VPN IPSEC upd—IPSec connection information.
  - VPN CTCP upd—cTCP tunnel connection information.
  - VPN SDI upd—SDI AAA connection information.
  - VPN DHCP upd—Tunneled DHCP connection information.

If you do not enter a failover IP address, the **show failover** command displays 0.0.0.0 for the IP address, and monitoring of the interfaces remain in a “waiting” state. You must set a failover IP address for failover to work.

In multiple configuration mode, only the **show failover** command is available in a security context; you cannot enter the optional keywords.

## Examples

The following is sample output from the **show failover** command for Active/Standby Failover.

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan 101 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                Interface inside (10.130.9.3): Normal
                Interface outside (10.132.9.3): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                Interface inside (10.130.9.4): Normal
                Interface outside (10.132.9.4): Normal

Stateful Failover Logical Update Statistics
        Link : fover Vlan 101 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       1733
        Xmit Q:         0       2       15225
```

The following is sample output from the **show failover** command for Active/Active Failover.

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: third Vlan 101(up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                admin Interface outside (10.132.8.5): Normal
                admin Interface third (10.132.9.5): Normal
                admin Interface inside (10.130.8.5): Normal
                admin Interface fourth (10.130.9.5): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)

                admin Interface outside (10.132.8.6): Normal
                admin Interface third (10.132.9.6): Normal
                admin Interface inside (10.130.8.6): Normal
                admin Interface fourth (10.130.9.6): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal
```

```
Stateful Failover Logical Update Statistics
        Link : third Vlan 101 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config failover** | Displays the **failover** commands in the current configuration. |

# show file

To display information about the file system, use the **show file** command in privileged EXEC mode.

**show file descriptors | system | information** *filename*

## Syntax Description

| | |
|---|---|
| **descriptors** | Displays all open file descriptors. |
| information | Displays information about a specific file. |
| *filename* | Specifies the filename. |
| **system** | Displays the size, bytes available, type of media, flags, and prefix information about the disk file system. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | Support for this command was introduced. |

## Examples

The following example shows how to display the file system information:

```
hostname# show file descriptors
No open file descriptors
hostname# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

## Related Commands

| Command | Description |
|---|---|
| **dir** | Displays the directory contents. |
| **pwd** | Displays the current working directory. |

# show firewall

To show the current firewall mode (routed or transparent), use the **show firewall** command in privileged EXEC mode.

**show firewall**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 2.2(1) | This command was introduced. |
| 3.1(1) | In the system execution space, this command now shows the firewall mode for each context. You can now set the firewall mode independently for each context. |

## Examples

The following is sample output from the **show firewall** command in single mode or within a context:

```
hostname# show firewall
Firewall mode: Router
```

The following is sample output from the **show firewall** command within a context:

```
hostname# show firewall

Context      Mode
-------------------------
customerA    Transparent
customerB    Routed
```

## Related Commands

| Command | Description |
|---|---|
| **firewall transparent** | Sets the firewall mode. |
| **show mode** | Shows the current context mode, either single or multiple. |

# show firewall autostate (IOS)

To view the setting of the autostate feature, use the **show firewall autostate** command in privileged EXEC mode. Autostate messaging in Cisco IOS software allows the FWSM to quickly detect that a switch interface has failed or come up.

**show firewall autostate**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, autostate is disabled.

## Command Modes

Privileged EXEC.

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXF5 | This command was introduced. |

## Usage Guidelines

The switch supervisor sends an autostate message to the FWSM when:

- The last interface belonging to a VLAN goes down.
- The first interface belonging to a VLAN comes up.

## Related Commands

| Command | Description |
|---|---|
| **firewall autostate** | Enables the autostate feature. |

# show firewall module (IOS)

To view the VLAN groups assigned to each FWSM, enter the **show firewall module** command in privileged EXEC mode.

**show firewall module** [*module_number*]

## Syntax Description

| | |
|---|---|
| *module_number* | (Optional) Specifies the module number. Use the **show module** command to view installed modules and their numbers. |

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC mode.

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Examples

The following is sample output from the **show firewall module** command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

## Related Commands

| Command | Description |
|---|---|
| **firewall module** | Assigns a VLAN group to an FWSM. |
| **firewall vlan-group** | Assigns VLANs to a VLAN group. |
| **show firewall vlan-group** | Shows the VLAN groups and the VLANs assigned to them. |
| **show module** | Shows all installed modules. |

# show firewall module state (IOS)

To view the state of each FWSM, enter the **show firewall module state** command in privileged EXEC mode.

**show firewall module** [*module_number*] **state**

## Syntax Description

| | |
|---|---|
| *module_number* | (Optional) Specifies the module number. |

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC mode.

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Examples

The following is sample output from the **show firewall module state** command:

```
Router# show firewall module 11 state
Firewall module 11:

Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
     501-505,913,972
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

## Related Commands

| Command | Description |
|---|---|
| **firewall module** | Assigns a VLAN group to an FWSM. |
| **firewall vlan-group** | Assigns VLANs to a VLAN group. |
| **show firewall vlan-group** | Shows the VLAN groups and the VLANs assigned to them. |
| **show module** | Shows all installed modules. |

# show firewall module traffic (IOS)

To view the traffic flowing through each FWSM, enter the **show firewall module traffic** command in privileged EXEC mode.

**show firewall module** [*module_number*] **traffic**

## Syntax Description

| | |
|---|---|
| *module_number* | (Optional) Specifies the module number. |

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC mode.

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Examples

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

```
Router# show firewall module 11 traffic
Firewall module 11:

Specified interface is up line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
     8709 packets input, 845553 bytes, 0 no buffer
     Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     18652077 packets output, 1480488712 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

## Related Commands

| Command | Description |
|---|---|
| **firewall module** | Assigns a VLAN group to an FWSM. |
| **firewall vlan-group** | Assigns VLANs to a VLAN group. |
| **show firewall vlan-group** | Shows the VLAN groups and the VLANs assigned to them. |
| **show module** | Shows all installed modules. |

# show firewall vlan-group (IOS)

To view VLAN groups that can be assigned to the FWSM, enter the **show firewall vlan-group** command in privileged EXEC mode.

**show firewall vlan-group** [*firewall_group*]

## Syntax Description

| | |
|---|---|
| *firewall_group* | (Optional) Specifies the group ID. |

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC mode.

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Examples

The following is sample output from the **show firewall vlan-group** command:

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

## Related Commands

| Command | Description |
|---|---|
| **firewall module** | Assigns a VLAN group to an FWSM. |
| **firewall vlan-group** | Creates a group of VLANs. |
| **show module** | Shows all installed modules. |

# show fragment

To display the operational data of the IP fragment reassembly module, enter the **show fragment** command in privileged EXEC mode.

**show fragment** [*interface*]

## Syntax Description

| | |
|---|---|
| *interface* | (Optional) Specifies the FWSM interface. |

## Defaults

If an *interface* is not specified, the command applies to all interfaces.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Privileged EXEC mode | • | • | • | • | |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |
| 3.1(1) | The command was separated into two commands, **show fragment** and **show running-config fragment**, to separate the configuration data from the operational data. |

## Examples

This example shows how to display the operational data of the IP fragment reassembly module:

```
hostname# show fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure fragment** | Clears the IP fragment reassembly configuration and resets the defaults. |
| **clear fragment** | Clears the operational data of the IP fragment reassembly module. |
| **fragment** | Provides additional management of packet fragmentation and improves compatibility with NFS. |
| **show running-config fragment** | Displays the IP fragment reassembly configuration. |

# show gc

To display the garbage collection process statistics, use the **show gc** command in privileged EXEC mode.

**show gc**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behaviors or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Examples

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

```
hostname# show gc

Garbage collection process stats:
Total tcp conn delete response          :            0
Total udp conn delete response          :            0
Total number of zombie cleaned          :            0
Total number of embryonic conn cleaned  :            0
Total error response                    :            0
Total queries generated                 :            0
Total queries with conn present response  :          0
Total number of sweeps                  :          946
Total number of invalid vcid            :            0
Total number of zombie vcid             :            0
```

## Related Commands

| Command | Description |
|---|---|
| **clear gc** | Removes the garbage collection process statistics. |

# show h225

To display information for H.225 sessions established across the FWSM, use the **show h225** command in privileged EXEC mode.

**show h225**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Usage Guidelines

The **show h225** command displays information for H.225 sessions established across the FWSM. Along with the **debug h323 h225 event**, **debug h323 h245 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

Before using the **show h225**, **show h245**, or **show h323-ras** commands, we recommend that you configure the **pager** command. If there are a lot of session records and the **pager** command is not configured, it may take a while for the **show** output to reach its end. If there is an abnormally large number of connections, check that the sessions are timing out based on the default timeout values or the values set by you. If they are not, then there is a problem that needs to be investigated.

## Examples

The following is sample output from the **show h225** command:

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
 | Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
 | 1. CRV 9861
 | Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
 | Local: | 10.130.56.4/1050 | Foreign: 172.30.254.205/1720
```

This output indicates that there is currently 1 active H.323 call going through the FWSM between the local endpoint 10.130.56.3 and foreign host 172.30.254.203, and for these particular endpoints, there is 1 concurrent call between them, with a CRV (Call Reference Value) for that call of 9861.

For the local endpoint 10.130.56.4 and foreign host 172.30.254.205, there are 0 concurrent Calls. This means that there is no active call between the endpoints even though the H.225 session still exists. This could happen if, at the time of the **show h225** command, the call has already ended but the H.225 session has not yet been deleted. Alternately, it could mean that the two endpoints still have a TCP connection opened between them because they set "maintainConnection" to TRUE, so that the session is kept open until they set it to FALSE again, or until the session times out based on the H.225 timeout value in your configuration.

## Related Commands

| Commands | Description |
|---|---|
| **debug h323** | Enables the display of debug information for H.323. |
| **inspect h323** | Enables H.323 application inspection. |
| **show h245** | Displays information for H.245 sessions established across the FWSM by endpoints using slow start. |
| **show h323-ras** | Displays information for H.323 RAS sessions established across the FWSM. |
| **timeout** | Configures the idle timeouts related to H.225 and H.323. |

# show h245

To display information for H.245 sessions established across the FWSM by endpoints using slow start, use the **show h245** command in privileged EXEC mode.

**show h245**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Usage Guidelines

The **show h245** command displays information for H.245 sessions established across the FWSM by endpoints using slow start. (Slow start is when the two endpoints of a call open another TCP control channel for H.245. Fast start is where the H.245 messages are exchanged as part of the H.225 messages on the H.225 control channel.) Along with the **debug h323 h245 event**, **debug h323 h225 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

## Examples

The following is sample output from the **show h245** command:

```
hostname# show h245
Total: 1
|LOCAL|TPKT|FOREIGN|TPKT
1|10.130.56.3/1041|0|172.30.254.203/1245|0
|MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
|Local|10.130.56.3 RTP 49608 RTCP 49609
|MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
|Local|10.130.56.3 RTP 49606 RTCP 49607
```

There is currently one H.245 control session active across the FWSM. The local endpoint is 10.130.56.3, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0. (The TKTP header is a 4-byte header preceding each H.225/H.245 message. It gives the length of the message, including the 4-byte header.) The foreign host endpoint is 172.30.254.203, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0.

The media negotiated between these endpoints have a LCN (logical channel number) of 258 with the foreign RTP IP address/port pair of 172.30.254.203/49608 and a RTCP IP address/port of 172.30.254.203/49609 with a local RTP IP address/port pair of 10.130.56.3/49608 and a RTCP port of 49609.

The second LCN of 259 has a foreign RTP IP address/port pair of 172.30.254.203/49606 and a RTCP IP address/port pair of 172.30.254.203/49607 with a local RTP IP address/port pair of 10.130.56.3/49606 and RTCP port of 49607.

## Related Commands

| Commands | Description |
|---|---|
| **debug h323** | Enables the display of debug information for H.323. |
| **inspect h323** | Enables H.323 application inspection. |
| **show h245** | Displays information for H.245 sessions established across the FWSM by endpoints using slow start. |
| **show h323-ras** | Displays information for H.323 RAS sessions established across the FWSM. |
| **timeout** | Configures the idle timeouts related to H.225 and H.323. |

# show h323

To display information for H.323 RAS or GUP sessions established across the FWSM between a gatekeeper and its H.323 endpoint, use the **show h323** command in privileged EXEC mode.

**show h323** [**gup** | **ras**]

## Syntax Description

| | |
|---|---|
| **gup** | Displays the GUP session information. |
| **ras** | Displays the RAS session information. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.2(1) | This command was introduced. |

## Usage Guidelines

The **show h323** command displays information for H.323 RAS or GUP sessions established across the FWSM between a gatekeeper and its H.323 endpoint. Along with the **debug h323 ras event** and **show local-host** commands, this command is used for troubleshooting H.323 RAS inspection engine issues.

The **show h323** command displays connection information for troubleshooting H.323 inspection engine issues, and is described in the **inspect protocol h323 {h225 | ras**} command page.

## Examples

The following is sample output from the **show h323** command:

```
hostname# show h323 gup
No  Local              Foreign
1   inside:100.0.07/8549outside:100.0.0.6/35510
```

## Related Commands

| Commands | Description |
|---|---|
| **debug h323** | Enables the display of debug information for H.323. |
| **inspect h323** | Enables H.323 application inspection. |
| **show h245** | Displays information for H.245 sessions established across the FWSM by endpoints using slow start. |

| Commands | Description |
|---|---|
| **show h323-ras** | Displays information for H.323 RAS sessions established across the FWSM. |
| **timeout** | Configures the idle timeouts related to H.225 and H.323. |

# show history

To display the previously entered commands, use the **show history** command in user EXEC mode.

**show history**

### Syntax Description

This command has no arguments or keywords.

### Defaults

No default behavior or values.

### Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| User EXEC | • | • | • | • | • |

### Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

### Usage Guidelines

The **show history** command lets you display previously entered commands. You can examine commands individually with the up and down arrows, enter **^p** to display previously entered lines, or enter **^n** to display the next line.

### Examples

The following example shows how to display previously entered commands when you are in user EXEC mode:

```
hostname> show history
    show history
    help
    show history
```

The following example shows how to display previously entered commands in privileged EXEC mode:

```
hostname# show history
    show history
    help
    show history
    enable
    show history
```

This example shows how to display previously entered commands in global configuration mode:

```
hostname(config)# show history
    show history
    help
```

```
show history
enable
show history
config t
show history
```

## Related Commands

| Command | Description |
|---|---|
| **help** | Displays help information for the command specified. |

# show idb

To display information about the status of interface descriptor blocks, use the **show idb** command in privileged EXEC mode.

**show idb**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| User EXEC | • | • | • | — | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

IDBs are the internal data structure representing interface resources. See the **Examples** section for a description of the display output.

## Examples

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

```
hostname# show idb
Maximum number of Software IDBs 16464.  In use 14.

                   HWIDBs      SWIDBs
             Active 3          13
           Inactive 1          1
         Total IDBs 4          14
 Size each (bytes) 156        260
        Total bytes 624        3640

HWIDB#  1 0x2e63b40  EOBC
HWIDB#  2 0x2e4fd00  Vlan
HWIDB#  3 0x2e5f670  Vlan

SWIDB#  1 0x02e4fdc8 0xffffffff Vlan UP UP
SWIDB#  2 0x04b97970 0xffffffff Vlan20 UP UP
SWIDB#  3 0x04b98c58 0xffffffff Vlan22 UP UP
SWIDB#  4 0x04b98e48 0xffffffff Vlan34 UP UP
SWIDB#  5 0x04b99038 0xffffffff Vlan35 UP UP
SWIDB#  6 0x04b99228 0xffffffff Vlan36 UP UP
```

```
SWIDB#  7 0x04b99418 0xffffffff Vlan37 UP UP
SWIDB#  8 0x04b99608 0xffffffff Vlan38 UP UP
SWIDB#  9 0x04b997f8 0xffffffff Vlan124 UP UP
SWIDB# 10 0x04b999f8 0xffffffff Vlan136 UP UP
SWIDB# 11 0x04b99bf8 0xffffffff Vlan137 UP UP
SWIDB# 12 0x02e5f738 0xffffffff Vlan UP UP
SWIDB# 13 0x02e63c08 0x00000103 EOBC UP UP
```

Fields and description are as follows:

| 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 interface in the system, and for each interface that is allocated to a context.<br>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 |
|---|---|
| **interface** | Configures an interface and enters interface configuration mode. |
| **show interface** | Displays the runtime status and statistics of interfaces. |

# show igmp groups

To display the multicast groups with receivers that are directly connected to the FWSM and that were learned through IGMP, use the **show igmp groups** command in privileged EXEC mode.

**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. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(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:

```
hostname# 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 in privileged EXEC mode.

**show igmp interface** [*if_name*]

## Syntax Description

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

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Privileged EXEC | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(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:

```
hostname# 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 FWSM and that were learned through IGMP. |

# show igmp traffic

To display IGMP traffic statistics, use the **show igmp traffic** command in privileged EXEC mode.

**show igmp traffic**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Examples

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

```
hostname# 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 interface

To display the information about the VLAN configuration, use the **show interface** command in privileged EXEC mode.

**show interface** [*interface_name*] [**detail** | **stats** | {**ip** [**brief**]}]

## Syntax Description

| | |
|---|---|
| *interface_name* | (Optional) Identifies the interface name set with the **nameif** command. |
| **detail** | (Optional) Displays the interface configuration details. |
| **stats** | (Optional) Displays the interface statistics. |
| **ip** | (Default) Displays information about the interface IP configuration. |
| **brief** | (Optional) Displays compacted information about the interface IP configuration. |

## Defaults

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

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |
| 3.1(1) | This command was modified to include the new interface numbering scheme, and to add the **stats** keyword for clarity, and the **detail** keyword. |

## Usage Guidelines

You can use this command to display the status of interfaces. You can specify the ID (as either the VLAN or the mapped name) or the name of the interface.

The dropped packets statistic in the display shows a record of those packets that arrived on the interface, but were not destined for the FWSM. These packets include traffic flooded by the switch, multicast and broadcast traffic (unless the FWSM is configured to relay those) and packets that fail sanity checks such as incorrect IP length versus Layer 2 length or checksums. This counter does not record packets dropped by the security policy.

**Note** The **show interface** command only shows interfaces you have configured using the **interface vlan** command; it does not show VLANs assigned to the FWSM that you have not yet configured. To view all VLANs assigned to the FWSM, use the **show vlan** command.

## Examples

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

```
hostname# show interface
Interface Vlan20 "outsidedmz", is down, line protocol is down
        MAC address 000f.90d7.1a00, MTU 1500
        IP address 10.0.0.1, subnet mask 255.0.0.0
  Traffic Statistics for "outsidedmz":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
Interface Vlan55 "inside", is up, line protocol is up
        MAC address 000f.90d7.1a00, MTU 1500
        IP address 192.168.62.20, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
        14582034 packets input, 2171077656 bytes
        406297 packets output, 243028833 bytes
        14812043 packets dropped
Interface Vlan56 "outside", is up, line protocol is up
        MAC address 000f.90d7.1a00, MTU 1500
        IP address 10.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "outside":
        0 packets input, 0 bytes
        33 packets output, 2244 bytes
        569730 packets dropped
Interface Vlan80 "", is up, line protocol is up
        Available but not configured via nameif
```

Field descriptions for the **show interface** command are shown below:

| Field | Description |
|---|---|
| Interface *ID* | The interface ID. Within a context, the FWSM shows the mapped name (if configured), unless you set the **allocate-interface** command **visible** keyword. |
| “*interface_name*” | The interface name set with the **nameif** command. In the system execution space, this field is blank because you cannot set the name in the system. If you do not configure a name, the following message appears after the Hardware line:<br>`Available but not configured via nameif` |
| is *state* | The administrative state, as follows:<br>• up—The interface is not shut down.<br>• administratively down—The interface is shut down with the **shutdown** command. |
| Line protocol is *state* | The line status, as follows:<br>• up—A working cable is plugged into the network interface.<br>• down—Either the cable is incorrect or not plugged into the interface connector. |
| *message area* | A message might be displayed in some circumstances. See the following examples:<br>• In the system execution space, you might see the following message:<br>`Available for allocation to a context`<br>• If you do not configure a name, you see the following message:<br>`Available but not configured via nameif` |

| Field | Description |
|---|---|
| MAC address | The interface 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 set using the **ip address** command or received from a DHCP server. In the system execution space, this field shows “IP address unassigned” because you cannot set the IP address in the system. |
| Subnet mask | The subnet mask for the IP address. |
| 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. |

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

```
hostname# show interface detail
Interface Vlan20 "outsidedmz", is down, line protocol is down
        MAC address 000f.90d7.1a00, MTU 1500
        IP address 10.0.0.1, subnet mask 255.0.0.0
  Traffic Statistics for "outsidedmz":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is not active
  Control Point Vlan20 States:
        Interface vlan config status is not active
        Interface vlan state is UP
Interface Vlan55 "inside", is up, line protocol is up
        MAC address 000f.90d7.1a00, MTU 1500
        IP address 172.23.62.20, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
        14582811 packets input, 2171191886 bytes
        406469 packets output, 243041933 bytes
        14812823 packets dropped
  Control Point Interface States:
        Interface number is 2
        Interface config status is active
        Interface state is active
  Control Point Vlan55 States:
        Interface vlan config status is active
        Interface vlan state is UP
Interface Vlan56 "outside", is up, line protocol is up
        MAC address 000f.90d7.1a00, MTU 1500
        IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "outside":
        0 packets input, 0 bytes
        33 packets output, 2244 bytes
        570042 packets dropped
  Control Point Interface States:
        Interface number is 3
        Interface config status is active
        Interface state is active
  Control Point Vlan56 States:
        Interface vlan config status is active
        Interface vlan state is UP
  Asymmetrical Routing Statistics:
        Received 0 packets
        Transmitted 163 packets
        Dropped 0 packets
Interface Vlan80 "", is up, line protocol is up
        Available but not configured via nameif
```

Each field description for the **show interface detail** command is shown below.

| Field | Description |
|---|---|
| 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:<br>• active—The interface is not shut down.<br>• not active—The interface is shut down with the **shutdown** command. |
| 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 FWSM brings the interfaces up or down as needed. |
| Control Point *vlan* States: | |
| Interface vlan config status | The administrative state, as follows:<br>• active—The interface is not shut down.<br>• not active—The interface is shut down with the **shutdown** command. |
| Interface vlan 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 FWSM 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 |
|---|---|
| **allocate-interface** | Assigns interfaces and subinterfaces to a security context. |
| **clear interface** | Clears counters for the **show interface** command. |
| **interface** | Configures an interface and enters interface configuration mode. |
| **nameif** | Sets the interface name. |
| **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 in privileged EXEC mode.

**show interface** [**interface** *interface_name*] **ip brief**

## Syntax Description

| | |
|---|---|
| **interface** *interface_name* | (Optional) Identifies the interface name set with the **nameif** command. |
| **ip brief** | (Optional) Displays compacted information about the interface IP configuration. |

## Defaults

If you do not specify an interface, the FWSM shows all interfaces.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name or the interface name in a context.

## Examples

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

```
hostname# show interface ip brief
Interface                  IP-Address      OK? Method  Status                Protocol
Vlan10 209.165.200.226 YES CONFIG  up                    up
Vlan40 unassigned      YES unset   administratively down down
Vlan41 10.1.1.50       YES manual  administratively down down
Vlan42 192.168.2.6     YES DHCP    administratively down down
```

The field descriptions for the **show interface ip brief** command are as follows:

| Field | Description |
|---|---|
| Interface | The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command. |
| IP-Address | The interface IP address. |
| OK? | This column is not currently used, and always shows "Yes." |
| Method | The method by which the interface received the IP address. Values include the following:<br>• unset—No IP address configured.<br>• manual—Configured the running configuration.<br>• CONFIG—Loaded from the startup configuration.<br>• DHCP—Received from a DHCP server. |
| Status | The administrative state, as follows:<br>• up—The interface is not shut down.<br>• administratively down—The interface is shut down with the **shutdown** command. |
| Protocol | The line status, as follows:<br>• up—A working cable is plugged into the network interface.<br>• down—Either the cable is incorrect or not plugged into the interface connector. |

## Related Commands

| Command | Description |
|---|---|
| **allocate-interface** | Assigns interfaces and subinterfaces to a security context. |
| **interface** | Configures an interface and enters interface configuration mode. |
| **ip address** | Sets the IP address for the interface or sets the management IP address for a transparent firewall. |
| **nameif** | Sets the interface name. |
| **show interface** | Displays the runtime status and statistics of interfaces. |

# show ip address

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

**show ip address [interface** *interface_name*]

## Syntax Description

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

## Defaults

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

## Command Modes

The following table shows the modes in which you can enter the command:

| | **Firewall Mode** | | **Security Context** | | |
|---|---|---|---|---|---|
| | | | | **Multiple** | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Privileged EXEC | • | • | • | • | — |

## Command History

| **Release** | **Modification** |
|---|---|
| 1.1(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.

## Examples

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

```
hostname# show ip address
System IP Addresses:
Interface                Name         IP address      Subnet mask       Method
Vlan20        mgmt         10.7.12.100     255.255.255.0     CONFIG
Vlan22        inside       10.1.1.100      255.255.255.0     CONFIG
Vlan34        outside      209.165.201.2   255.255.255.224   DHCP
Vlan35        dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface                Name         IP address      Subnet mask       Method
Vlan36       mgmt         10.7.12.100     255.255.255.0     CONFIG
Vlan37       inside       10.1.1.100      255.255.255.0     CONFIG
Vlan38       outside      209.165.201.2   255.255.255.224   DHCP
Vlan124       dmz          209.165.200.225 255.255.255.224   manual
```

The current IP addresses are the same as the system IP addresses on the failover active module. When the primary module fails, the current IP addresses become the IP addresses of the standby module.

The field descriptions for the **show ip address** command are as follows:

| Field | Description |
|---|---|
| Interface | The interface ID. |
| Name | The interface name set with the **nameif** command. |
| 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:<br>• unset—No IP address configured.<br>• manual—Configured the running configuration.<br>• CONFIG—Loaded from the startup configuration.<br>• DHCP—Received from a DHCP server. |

## Related Commands

| Command | Description |
|---|---|
| **allocate-interface** | Assigns interfaces and subinterfaces to a security context. |
| **interface** | Configures an interface and enters interface configuration mode. |
| **nameif** | Sets the interface name. |
| **show interface** | Displays the runtime status and statistics of interfaces. |
| **show interface ip brief** | Shows the interface IP address and status. |

# show ip bgp neighbors

To display information about the TCP and BGP connections to neighbors, use the **show ip bgp neighbors** command in privileged EXEC mode.

**show ip bgp neighbors**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context[1] | System |
| Privileged EXEC | • | — | • | • | — |

[1] This command is only available in the admin context.

## Command History

| Release | Modification |
|---|---|
| 3.2(1) | This command was introduced. |

## Usage Guidelines

Use the **show ip bgp neighbors** command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

## Examples

The following is sample output from the **show ip bgp neighbors** command.

```
hostname# show ip bgp neighbors

BGP neighbor is 10.6.20.10,  remote AS 100, internal link
  BGP version 4, remote router ID 120.1.1.1
  BGP state = Established, up for 00:09:18
  Last read 00:00:20, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                        Sent       Rcvd
    Opens:          1          1
    Notifications:  0          0
    Updates:        1          0
    Keepalives:     12         11
    Route Refresh:  0          0
    Total:          14         13
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  neighbor version 1
  Index 0, Offset 0, Mask 0x0
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:      0          0
    Prefixes Total:        0          0
    Implicit Withdraw:     0          0
    Explicit Withdraw:     0          0
    Used as bestpath:      n/a        0
    Used as multipath:     n/a        0
  Number of NLRIs in the update sent: max 1, min 0

  Connections established 1; dropped 0
  Last reset never
```

Table 26-7 describes the significant fields shown in the display. Fields that are preceded by the asterisk character are displayed only when the counter has a non-zero value.

*Table 26-7 The show ip bgp neighbors Command Field Descriptions*

| Field | Description |
|---|---|
| BGP neighbor | IP address of the BGP neighbor and its autonomous system number. |
| remote AS | Autonomous-system number of the neighbor. |
| internal link | “internal link” is displayed for iBGP neighbors. “external link” is displayed for eBGP neighbors. For BGP stub routing, only iBGP is supported. |
| BGP version | BGP version being used to communicate with the remote router. |
| remote router ID | IP address of the neighbor. |
| BGP state | Finite state machine (FSM) stage of session negotiation. |
| up for | Time, in seconds, that the underlying TCP connection has been in existence. |
| Last read | Time since BGP last received a message from this neighbor. |
| hold time | Time, in seconds, that BGP will maintain the session with this neighbor without receiving a messages. |
| keepalive interval | Time, interval in seconds, that keepalive messages are transmitted to this neighbor. |
| Neighbor capabilities | BGP capabilities advertised and received from this neighbor. “Advertised and received” is displayed when a capability is successfully exchanged between two routers. |
| Route Refresh | Status of the route refresh capability. |
| Address family IPv4 Unicast | IP Version 4 unicast-specific properties of this neighbor. |
| Message statistics | Statistics organized by message type. |

*Table 26-7 The show ip bgp neighbors Command Field Descriptions (continued)*

| Field | Description |
|---|---|
| InQ depth is | Number of messages in the input queue. |
| OutQ depth is | Number of messages in the output queue. |
| Sent | Total number of transmitted messages. |
| Received | Total number of received messages. |
| Opens | Number of open messages sent and received. |
| notifications | Number of notification (error) messages sent and received. |
| Updates | Number of update messages sent and received. |
| Keepalives | Number of keepalive messages sent and received. |
| Route Refresh | Number of route refresh request messages sent and received. |
| Total | Total number of messages sent and received. |
| Default minimum time between... | Time, in seconds, between advertisement transmissions. |
| For address family: | Address family for which the following fields refer. |
| neighbor version | Number used by Cisco IOS to track prefixes that have been sent and those that need to be sent. |
| Prefix activity | Prefix statistics for this address family. |
| Prefixes current | Number of prefixes accepted for this address family. |
| Prefixes total | Total number of received prefixes. |
| Implicit Withdraw | Number of times that a prefix has been withdrawn and readvertised. |
| Explicit Withdraw | Number of times that prefix is withdrawn because it is no longer feasible. |
| Used as bestpath | Number of received prefixes installed as a best paths. |
| Used as multipath | Number of received prefixes installed as multipaths. |
| Number of NLRIs... | Number of network layer reachability attributes in updates. |
| Connections established | Number of times a TCP and BGP connection have been successfully established. |
| dropped | Number of times that a valid session has failed or been taken down. |
| Last reset | Time since this peering session was last reset. The reason for the reset is displayed on this line. |

## Related Commands

| Command | Description |
|---|---|
| **neighbor** | Specifies the BGP neighbor. |
| **router bgp** | Creates a BGP routing process and enters router configuration mode for that process. |
| **show running-config router** | Displays the router commands in the running configuration. |

# show ip bgp neighbors advertised-routes

To display the routes that are advertised to the BGP neighbor, use the **show ip bgp neighbors advertised-routes** command in privileged EXEC mode.

**show ip bgp neighbors advertised-routes**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context[1] | System |
| Privileged EXEC | • | — | • | • | — |

[1] This command is only available in the admin context.

## Command History

| Release | Modification |
|---|---|
| 3.2(1) | This command was introduced. |

## Usage Guidelines

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

## Examples

The following example displays routes advertised for the BGP neighbor:

```
hostname# show ip bgp neighbors advertised-routes

local router ID is 5.6.7.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  171.0.0.0/8      10.6.37.124              0    100 32768  i
```

Table 26-8describes the fields shown in the display.

*Table 26-8 The show ip bgp neighbors advertised-routes Field Information*

| Field | Description |
|---|---|
| local router ID | The router ID of the FWSM. In order of precedence and availability, the router ID specified by the **bgp router-id** command or the highest IP address. |
| Status codes | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:<br>s—The table entry is suppressed.<br>d—The table entry is dampened and will not be advertised to BGP neighbors.<br>h—The table entry does not contain the best path based on historical information.<br>*—The table entry is valid.<br>>—The table entry is the best entry to use for that network.<br>i—The table entry was learned via an iBGP session. |
| Origin codes | Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:<br>i—Entry originated from IGP and was advertised with a network router configuration command.<br>e—Entry originated from EGP.<br>?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |
| Network | IP address of a network. |
| Next Hop | IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network. |
| Metric | If shown, this is the value of the inter-autonomous system metric. This field is not used frequently. |
| LocPrf | Local preference value as set with the set **local-preference route-map** configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |

## Related Commands

| Command | Description |
|---|---|
| **network** | Defines the networks that can be advertised by the BGP routing process. |
| **router bgp** | Creates a BGP routing process and enters router configuration mode for that process. |

# show ip bgp summary

To display the status of the BGP connection, use the **show ip bgp summary** command in privileged EXEC mode.

**show ip bgp summary**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context[1] | System |
| Privileged EXEC | • | — | • | • | — |

[1] This command is only available in the admin context.

## Command History

| Release | Modification |
|---|---|
| 3.2(1) | This command was introduced. |

## Usage Guidelines

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

## Examples

The following is sample output from the **show ip bgp summary** command.

```
hostname# show ip bgp summary

BGP router identifier 5.6.7.8, local AS number 100

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
     10.6.20.10 4 100   7       8       1        0    0    00:03:50 (NoNeg)
```

Table 26-9 describes the significant fields shown in the display. Fields that are preceded by the asterisk character are not shown in the preceding output.

*Table 26-9 The show ip bgp summary Command Field Descriptions*

| Field | Description |
|---|---|
| BGP router identifier | In order of precedence and availability, the router identifier specified by the **bgp router-id** command or the highest IP address. |
| local AS number | The autonomous system number of the FWSM. |
| Neighbor | IP address of the neighbor. |
| V | BGP version number spoken to the neighbor. |
| AS | Autonomous system number. |
| MsgRcvd | Number of messages received from the neighbor. |
| MsgSent | Number of messages sent to the neighbor. |
| TblVer | Last version of the BGP database that was sent to the neighbor. |
| InQ | Number of messages queued to be processed from the neighbor. |
| OutQ | Number of messages queued to be sent to the neighbor. |
| Up/Down | The length of time that the BGP session has been in the Established state, or the current status if not in the Established state. |
| State/PfxRcd | Current state of the BGP session, and the number of prefixes that have been received from a neighbor. |

## Related Commands

| Command | Description |
|---|---|
| **neighbor** | Specifies the BGP neighbor. |
| **network** | Specifies the networks that can be advertised by the BGP routing process. |
| **router bgp** | Creates a BGP routing process and enters router configuration mode for that process. |
| **show running-config router** | Displays the **router** commands in the running configuration. |

# show ip nbar protocol-tagging (IOS)

If you use Programmable Intelligent Services Accelerator (PISA) integration with the FWSM, then to view , use the **show ip nbar protocol-tagging** command in privileged EXEC mode.

**Note** This feature depends on Cisco IOS Release 12.2(18)ZYA, and will not be supported on the FWSM until the Cisco IOS software is released.

**show ip nbar protocol-tagging** {**key** | **interface** *ifname* | **summary**}

## Syntax Description

| | |
|---|---|
| **key** | Shows the GRE key used to tag the packets. |
| **interface** *ifname* | Shows if tagging is enabled on an interface. |
| **summary** | Shows a summary of the protocol tagging configuration. |

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC.

## Command History

| Release | Modification |
|---|---|
| 12.2(18)ZYA | This command was introduced. |

## Examples

The following is sample output from the **show ip nbar protocol-tagging summary** command:

```
Router# show ip nbar protocol-tagging summary
NBAR Tagging key:  0xFEEFABBA(default)
NBAR Tagging is enabled on the following interfaces:
       FastEthernet2/12
```

The following is sample output from the **show ip nbar protocol-tagging key** command:

```
Router# show ip nbar protocol-tagging key
NBAR Tagging key:  0xFEEFABBA(default)
```

The following is sample output from the **show ip nbar protocol-tagging interface** command:

```
Router# show ip nbar protocol-tagging interface FastEthernet 2/12
NBAR Tagging is enabled on this interface.
 vlan-list: 3,5,7-10
```

## Related Commands

| Command | Description |
|---|---|
| **ip nbar protocol-tagging (IOS)** | Enables protocol tagging. |

# show ip verify statistics

To show the number of packets dropped because of the Unicast RPF feature, use the **show ip verify statistics** command in privileged EXEC mode. Use the **ip verify reverse-path** command to enable Unicast RPF.

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

## Syntax Description

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

## Defaults

This command shows statistics for all interfaces.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced, |

## Examples

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

```
hostname# 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 configure ip verify reverse-path** | Clears the **ip verify reverse-path** configuration. |
| **clear ip verify statistics** | Clears the Unicast RPF statistics. |
| **ip verify reverse-path** | Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing. |
| **show running-config ip verify reverse-path** | Shows the **ip verify reverse-path** configuration. |

# show ipsec sa

To display a list of IPSec SAs, use the **show ipsec sa** command in global configuration mode or privileged EXEC mode. You can also use the alternate form of this command: **show crypto ipsec sa**.

**show ipsec sa** [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr* ] [**detail**]

## Syntax Description

| | |
|---|---|
| **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. |
| **map** *map-name* | (Optional) Displays IPSec SAs for the specified crypto map. |
| **peer** *peer-addr* | (Optional) Displays IPSec SAs for specified peer IP addresses. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Global configuration | • | • | • | — | — |
| Privileged EXEC | • | • | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Examples

The following example, entered in global configuration mode, displays IPSec SAs.

```
hostname(config)# 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
      #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 ={RA, Tunnel, }
         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 ={RA, Tunnel, }
         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)
hostname(config)#
```

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

```
hostname(config)# 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
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs for the keyword **entry**.

```
hostname(config)# 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
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs with the keywords **entry detail**.

```
hostname(config)# 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
hostname(config)#
```

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

```
hostname(config)# 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**.

```
hostname(config)# 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
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure isakmp** | Clears all the ISAKMP configuration. |
| **clear configure isakmp policy** | Clears all ISAKMP policy configuration. |
| **clear isakmp sa** | Clears the IKE runtime SA database. |
| **isakmp enable** | Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the FWSM. |
| **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 in global configuration mode or privileged EXEC mode.

**show ipsec sa summary**

## Syntax Description

This command has no arguments or variables.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | — | — |
| Privileged EXEC | • | • | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Examples

The following example, entered in global configuration mode, 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

```
hostname(config)# 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
hostname(config)#
```

## 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 in global configuration mode or privileged EXEC mode.

**show ipsec stats**

## Syntax Description

This command has no keywords or variables.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | — | — |
| Privileged EXEC | • | • | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Examples

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

```
hostname(config)# 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
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **clear ipsec sa** | Clears IPSec SAs or counters based on specified parameters. |
| **crypto ipsec transform-set** | Defines a transform set. |
| **show ipsec sa** | Displays IPSec SAs based on specified parameters. |
| **show ipsec sa summary** | Displays a summary of IPSec SAs. |

# show ipv6 access-list

To display the IPv6 access list, use the **show ipv6 access-list** command in privileged EXEC mode. The IPv6 access list determines what IPv6 traffic can pass through the FWSM.

**show ipv6 access-list** [*id* [*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*]]

## Syntax Description

| | |
|---|---|
| **any** | (Optional) An abbreviation for the IPv6 prefix ::/0. |
| **host**<br>*source-ipv6-address* | (Optional) IPv6 address of a specific host. When provided, only the access rules for the specified host are displayed. |
| *id* | (Optional) The access list name. When provided, only the specified access list is displayed. |
| *source-ipv6-prefix*<br>*/prefix-length* | (Optional) IPv6 network address and prefix. When provided, only the access rules for the specified IPv6 network are displayed. |

## Defaults

Displays all IPv6 access lists.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

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

## Examples

The following is sample output from the **show ipv6 access-list** command. It shows IPv6 access lists named inbound, tcptraffic, and outbound.

```
hostname# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
```

```
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

## Related Commands

| Command | Description |
|---|---|
| **ipv6 access-list** | Creates an IPv6 access list. |

# show ipv6 interface

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

**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, as designated by the **nameif** command. The status and configuration for only the designated interface is shown. |
| **prefix** | (Optional) Prefix generated from a local IPv6 prefix pool. |

## Defaults

Displays all IPv6 interfaces.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Privileged EXEC | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(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:

```
hostname# show ipv6 interface outside
interface Vlan101 "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:

```
hostname# 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.

```
hostname# 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 neighbor

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbor** command in privileged EXEC mode.

**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, as configure by the **nameif** command, only. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(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**—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**

  Interface from which the address was reachable.

### Examples

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

```
hostname# 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:

```
hostname# 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. |
| **ipv6 neighbor** | Configures a static entry in the IPv6 neighbor discovery cache. |

# show ipv6 route

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

**show ipv6 route**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## 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:

```
hostname# 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
```

## Related Commands

| Command | Description |
|---|---|
| **debug ipv6 route** | Displays debug messages for IPv6 routing table updates and route cache updates. |
| **ipv6 route** | Adds a static entry to the IPv6 routing table. |

# show ipv6 routers

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

**show ipv6 routers** [*if_name*]

## Syntax Description

| | |
|---|---|
| *if_name* | (Optional) The internal or external interface name, as designated by the **nameif** command, that you want to display information about. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(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:

```
hostname# 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 in privileged EXEC mode.

**show ipv6 traffic**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(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:

```
hostname# 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. |