THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2016–2018 Cisco Systems, Inc. All rights reserved.
Using the Command Line Interface (CLI)

The following topics explain how to use the command line interface (CLI) for Firepower Threat Defense (FTD) devices and how to interpret the command reference topics. Use the CLI for basic system setup and troubleshooting.

Note

When you deploy a configuration change using the Firepower Management Center or Firepower Device Manager, do not use the FTD CLI for long-running commands (such as ping with a huge repeat count or size); these commands could cause a deployment failure.

• Logging Into the Command Line Interface (CLI), on page 2
• Command Modes, on page 3
• Syntax Formatting, on page 5
• Entering Commands, on page 6
• Filtering Show Command Output, on page 7
• Command Help, on page 9
Logging Into the Command Line Interface (CLI)

To log into the CLI, use an SSH client to make a connection to the management IP address. Log in using the admin username (default password is Admin123) or another CLI user account.

You can also connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default. To enable SSH access, use the device manager (Firepower Management Center or Firepower Device Manager) to allow SSH connections to specific data interfaces. You cannot SSH to the Diagnostic interface.

You can create user accounts that can log into the CLI using the configure user add command. However, these users can log into the CLI only. They cannot log into the Firepower Device Manager web interface. The CLI supports local authentication only. You cannot access the CLI using external authentication.

Console Port Access

In addition to SSH, you can directly connect to the Console port on the device. Use the console cable included with the device to connect your PC to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control. See the hardware guide for your device for more information about the console cable.

The initial CLI you access on the Console port differs by device type.

• ASA Series devices—The CLI on the Console port is the regular FTD CLI.

• Firepower Series devices—The CLI on the Console port is FXOS. You can get to the FTD CLI using the connect ftd command. Use the FXOS CLI for chassis-level configuration and troubleshooting only. For the Firepower 2100, you cannot perform any configuration at the FXOS CLI. Use the FTD CLI for basic configuration, monitoring, and normal system troubleshooting. See the FXOS documentation for information on FXOS commands for the Firepower 4100 and 9300. See the Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series for information on FXOS commands for the Firepower 2100.
Command Modes

The CLI on a Firepower Threat Defense device has different modes, which are really separate CLIs rather than sub-modes to a single CLI. You can tell which mode you are in by looking at the command prompt.

Regular Firepower Threat Defense CLI

Use this CLI for Firepower Threat Defense management configuration and troubleshooting.

> 

Diagnostic CLI

Use this CLI for advanced troubleshooting. This CLI includes additional show and other commands, including the session wlan console command needed to enter the CLI for the wireless access point on an ASA 5506W-X. This CLI has two sub-modes; more commands are available in Privileged EXEC Mode.

To enter this mode, use the system support diagnostic-cli command in the Firepower Threat Defense CLI.

- User EXEC Mode. The prompt reflects the system hostname as defined in the running configuration.

    firepower>

- Privileged EXEC Mode. Enter the enable command to enter this mode (press enter without entering a password when prompted for a password).

    firepower#

Expert Mode

Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the expert command in the Firepower Threat Defense CLI.

The prompt is username@hostname if you log in using the admin user. If you use a different user, only the hostname is shown. The hostname is the name configured for the management interface. For example,

    admin@firepower:$

Firepower eXtensible Operating System (FXOS) CLI

On Firepower 2100, 4100, and 9300 series devices, FXOS is the operating system that controls the overall chassis. Depending on the model, you use FXOS for configuration and troubleshooting. From FXOS, you can enter the Firepower Threat Defense CLI using the connect ftd command.

For Firepower 2100 series devices, you can go from the Firepower Threat Defense CLI to the FXOS CLI using the connect fxos command.

The FXOS command prompt looks like the following, but the prompt changes based on mode. See the Cisco FXOS CLI Configuration Guide for your FXOS version and hardware model for details about FXOS CLI usage.
Firepower-module2>
Firepower-module2#
Syntax Formatting

Command syntax descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>command</strong></td>
<td><em>Command</em> text indicates commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><strong>variable</strong></td>
<td><em>Variable</em> text indicates arguments for which you supply values.</td>
</tr>
<tr>
<td><code>[x]</code></td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td>`[x</td>
<td>y]`</td>
</tr>
<tr>
<td>`{x</td>
<td>y}`</td>
</tr>
<tr>
<td>`[x {y</td>
<td>z}]`</td>
</tr>
</tbody>
</table>
**Entering Commands**

When you log into the CLI through the console port or an SSH session, you are presented with the following command prompt:

```>
```

You type the command at the prompt and press Enter to execute the command. Additional features include:

- **Scrolling through command history**—You can use the up and down arrow keys to scroll through the commands that you have already entered. You can reenter or edit and reenter the commands in the history.

- **Completing commands**—To complete a command or keyword after entering a partial string, press the space or Tab key. The partial string must match a single command or keyword only for it to be completed.

- **Abbreviating commands**—In the regular CLI, you cannot abbreviate commands. You must enter the full command string. However, in the diagnostic CLI, you can abbreviate most commands down to the fewest unique characters for a command; for example, you can enter `show ver` instead of `show version`.

- **Stopping command output**—If a command produces a lot of output, you can get out of it by pressing the q key.

- **Stopping long-running commands**—If a command is not returning output fast enough, and you want to try a different command, press Ctrl+C.
Filtering Show Command Output

You can filter the output of `show` commands by piping the output to filtering commands. Piping output works with all `show` commands but is most useful when dealing with commands that produce a lot of text.

To use the filtering capabilities, use the following format. In this case, the vertical bar `|` after the `show` command is the pipe character and is part of the command, not part of the syntax description. The filtering options come after the `|` character.

```
show command | {grep | include | exclude | begin} regular expression
```

Filtering Commands

You can use these filtering commands:

- **grep**—Display only those lines that match the pattern.
- **include**—Display only those lines that match the pattern.
- **exclude**—Exclude all lines that match the pattern, show all other lines.
- **begin**—Find the first line that includes the pattern, and display that line and all subsequent lines.

**regular_expression**

A regular expression, typically a simple text string. Do not enclose the expression in single or double-quotes, these will be seen as part of the expression. Also, trailing spaces will be included in the expression.

The following example shows how to change the output of the `show access-list` command to show only those rules that apply to the `inside1_2` interface.

```
> show access-list | include inside1_2
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
   rule-id 268435458
   event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
   rule-id 268435458
   event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
   rule-id 268435458
   event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
   rule-id 268435458
   event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
   rule-id 268435458
   event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
   rule-id 268435458
   event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
   rule-id 268435458
   event-log both (hitcnt=0) 0xc1579ed7
access-list NGFW_ONBOX_ACL line 10 advanced trust ip ifc inside1_4 any ifc inside1_2 any
   rule-id 268435458
   event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 11 advanced trust ip ifc inside1_5 any ifc inside1_2 any
   rule-id 268435458
```

Cisco Firepower Threat Defense Command Reference
event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x699725ea
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xda014e58
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457
event-log both (hitcnt=0) 0xea5bdd6e
Command Help

Help information is available from the command line by entering the following commands:

- ? to see a list of all commands.
- command_name ? to see the options for a command. For example, show ?.
- string? to show the commands or keywords that match the string. For example, n? shows all commands that start with the letter n.
- help command_name to see the syntax and limited usage information for a command. Enter help ? to see which commands have help pages.
PART I

A - R Commands

• a - clear e, on page 13
• clear f - clear z, on page 73
• clf - cz, on page 145
• d - r, on page 237
- clear e

  - aaa-server active, fail, on page 15
  - app-agent heartbeat, on page 16
  - asp inspect-dp egress-optimization, on page 18
  - asp load-balance per-packet, on page 19
  - asp packet-profile, on page 21
  - blocks, on page 22
  - capture, on page 24
  - capture-traffic, on page 31
  - clear aaa-server statistics, on page 36
  - clear access-list, on page 37
  - clear arp, on page 38
  - clear asp, on page 39
  - clear bfd, on page 41
  - clear bgp, on page 42
  - clear blocks, on page 45
  - clear capture, on page 46
  - clear clns, on page 47
  - clear cluster info, on page 48
  - clear configure key chain, on page 49
  - clear conn, on page 50
  - clear console-output, on page 52
  - clear counters, on page 53
  - clear cpu profile, on page 54
  - clear crashinfo, on page 55
  - clear crypto accelerator statistics, on page 56
  - clear crypto ca crls, on page 57
  - clear crypto ca trustpool, on page 58
  - clear crypto ikev1, on page 59
  - clear crypto ikev2, on page 60
  - clear crypto ipsec sa, on page 61
  - clear crypto isakmp, on page 63
  - clear crypto protocol statistics, on page 64
  - clear crypto ssl, on page 65
• clear dhcpd, on page 66
• clear dhcprelay statistics, on page 67
• clear dns, on page 68
• clear dns-hosts cache, on page 69
• clear eigrp events, on page 70
• clear eigrp neighbors, on page 71
• clear eigrp topology, on page 72
aaa-server active, fail

To reactivate a AAA server that is marked failed, use the `aaa-server active` command. To fail an active AAA server, use the `aaa-server fail` command.

```
aaa-server groupname { active | fail } host hostname
```

**Syntax Description**
- **active**: Sets the server to an active state.
- **fail**: Sets the server to a failed state.
- **hostname**: AAA server group or realm name.
- **host hostname**: FQDN or IP address of the server being acted upon.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Without this command, servers in a group that failed remain in a failed state until all servers in the group fail, after which all are reactivated. You can find the server group or realm name, as well as all the AAA server information in the output of the `show aaa-server` command.

**Examples**
The following example shows the state for server 192.168.125.60 in group1, and manuallyreactivates it:

```
> show aaa-server group1 host 192.68.125.60
Server Group: group1
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
Server status: FAILED. Server disabled at 11:10:08 UTC Fri Aug...
>
> aaa-server group1 active host 192.168.125.60
>
> show aaa-server group1 host 192.68.125.60
Server Group: group1
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC Fri Aug...
```

**Related Commands**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear aaa-server statistics</td>
<td>Clears AAA server statistics.</td>
</tr>
<tr>
<td>show aaa-server</td>
<td>Displays AAA server statistics</td>
</tr>
<tr>
<td>test aaa-server</td>
<td>Verify the configuration for a AAA server.</td>
</tr>
</tbody>
</table>
**app-agent heartbeat**

To configure the heartbeat message interval for the app-agent (application agent) running on the Firepower Threat Defense device on Firepower chassis, use the **app-agent heartbeat** command.

```
app-agent heartbeat [interval milliseconds] [retry-count integer]
```

**Syntax Description**

- **interval milliseconds**
  - Specifies the time interval in milliseconds between heartbeat messages. You can adjust the interval in increments of 100 milliseconds. The default is 1000. The allowed range is 100 to 6000 for release 6.2.2 and following, but 300 to 6000 for older releases.
  
  A loss of consecutive heartbeat messages up to the retry count triggers a failure notification to the rest of the system. The default of 1000 milliseconds provides an aggressive failure detection setting with the risk of false failure detections.

- **retry-count integer**
  - Specifies the number of times the app-agent should retry the heartbeat message if there is no response, or the app-agent receives an error response for the heartbeat message, from 3 to 10. The default is 3.

**Command Default**

The default interval value is 1000 milliseconds.

The default retry-count is 3.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.2</td>
<td>The allowed interval range was changed to 100 to 6000.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The primary responsibility of the app-agent running on the Firepower Threat Defense device is to interface and communicate between Firepower Threat Defense modules and the Firepower 2100, 4100, and 9300 FXOS chassis.

The heartbeat communication channel serves the purpose of monitoring the health of the link between the FXOS chassis and the Firepower Threat Defense application agent. The Firepower Threat Defense application sends request messages to the FXOS chassis supervisor at a certain interval, with retries at a set number of times until a proper response is received from the FXOS chassis supervisor.

The heartbeat mechanism between the Firepower Threat Defense app-agent and FXOS chassis supervisor also monitors the Hardware Bypass feature for failure. For certain interface modules on the Firepower 2100, 4100, and 9300, you can enable the Hardware Bypass feature. Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures.

**Examples**

The following example sets the app-agent heartbeat interval to 600 milliseconds and the retry count to 6 times:
app-agent heartbeat

```
> app-agent heartbeat interval 600 retry-count 6
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show app-agent</td>
<td>Shows the app-agent status.</td>
</tr>
<tr>
<td></td>
<td>show inline-set</td>
<td>Shows inline set information.</td>
</tr>
<tr>
<td></td>
<td>show interface</td>
<td>Shows interface status information.</td>
</tr>
</tbody>
</table>
asp inspect-dp egress-optimization

To enable egress optimization, use the `asp inspect-dp egress-optimization` command. To disable egress optimization, use the `no` form of this command.

Egress optimization is a performance feature targeted for selected IPS traffic. The feature is enabled by default on all FTD platforms.

**Note**

We strongly recommend you leave this feature enabled. Disable it only if advised to do so by Cisco TAC.

```
asp inspect-dp egress-optimization
no asp inspect-dp egress-optimization
```

**Command Default**

Egress optimization is enabled by default.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Egress optimization is intended to be enabled at all times to improve performance. Disable egress optimization only on the advice of Cisco TAC for troubleshooting purposes.

**Examples**

The following example shows how to enable egress optimization:

```
> asp inspect-dp egress-optimization
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show conn state egress_optimization</strong></td>
<td>Displays information about flows eligible for egress optimization. Use this command on the advice of Cisco TAC.</td>
</tr>
<tr>
<td><strong>show asp inspect-dp egress-optimization</strong></td>
<td>Show statistics related to egress optimization.</td>
</tr>
<tr>
<td><strong>clear asp inspect-dp egress-optimization</strong></td>
<td>Clear statistics related to egress optimization.</td>
</tr>
</tbody>
</table>
**asp load-balance per-packet**

To change the load balancing behavior on multiple cores to be per packet, use the `asp load-balance per-packet` command. To restore the default load-balancing mechanism, use the **no** form of this command.

**asp load-balance per-packet**

**no asp load-balance per-packet**

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per-packet load-balancing is disabled by default.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The job of the load balancer is to distribute packets to CPU cores and to maintain packet order. By default, a connection can only be processed by one core at a time. Due to this behavior, the cores will be under-utilized if there are a small number of interfaces/RX rings in use when compared to the number of cores. For example, if there are only two Gigabit Ethernet interfaces in use on a Firepower Threat Defense device, then only two cores will be used. (A Ten Gigabit Ethernet interface has 4 RX rings and a Gigabit Ethernet interface as 1 RX ring.) You may want to optimize the load balancer by enabling per-packet load balancing so you can use more cores.

The default load-balancing behavior optimizes overall system performance when you have many interfaces in use, while the per-packet load balancer optimizes the overall system performance when you have a smaller number of interfaces that are active.

If you enable per-packet load balancing, when one core processes packets from an interface, another core can receive and process the next packet from the same interface. Therefore, it is possible for all cores to process packets from the same interface simultaneously.

Per-packet load balancing will improve performance if:

- The system drops packets
- The **show cpu** command shows CPU usage far less than 100%—The CPU usage is a good indicator of how many cores are being used. For example, on an 8-core system, if two cores are used, **show cpu** shows 25%; four cores: 50%; six cores: 75%.
- There are a small number of interfaces that are in use

**Note**

Typically if there are less than 64 concurrent flows on the Firepower Threat Defense device, then enabling per-packet load balancing will incur more overhead than its benefit.

**Examples**

The following example shows how to change the default load-balancing behavior:

> `asp load-balance per-packet`
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clear asp load-balance</td>
<td>Clears and resets the ASP load balancing per packet history statistics. OK</td>
</tr>
<tr>
<td></td>
<td>show asp load-balance</td>
<td>Displays a histogram of the load balancer queue sizes. OK</td>
</tr>
</tbody>
</table>
asp packet-profile

To obtain statistics on how a Firepower Threat Defense device handles network traffic, use the `asp packet-profile` command. To disable packet profiling, use the `no` form of this command.

The Accelerated Security Path or ASP process determines how many packets were fastpathed by a prefilter policy, offloaded as a large flow, fully evaluated by access control (Snort), and so on.

```
asp packet-profile
no asp packet-profile
```

**Command Default**

Packet profiling is enabled by default.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Packet profiling is intended to be enabled at all times. If the CPU usage is high due to statistics collection and further computation, then the feature can be disabled.

**Examples**

The following example shows how to enable packet profiling:

```
> asp packet-profile
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show asp packet-profile</td>
<td>Displays statistics for the packets that traversed through dataplane only, the dataplane and Snort, and offloaded to hardware.</td>
</tr>
<tr>
<td>clear asp packet-profile</td>
<td>Clear statistics related to packet profiling.</td>
</tr>
</tbody>
</table>
blocks

To allocate additional memory to block diagnostics (displayed by the `show blocks` command), use the `blocks` command. To set the value back to the default, use the `no` form of this command.

```
blocks queue history enable [memory_size]
no blocks queue history enable [memory_size]
```

**Syntax Description**

- `memory_size` (Optional) Sets the memory size for block diagnostics in bytes, instead of applying the dynamic value. If this value is greater than free memory, an error message appears and the value is not accepted. If this value is greater than 50% of free memory, a warning message appears, but the value is accepted.

**Command Default**

The default memory assigned to track block diagnostics is 2136 bytes.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To view the currently allocated memory, enter the `show blocks queue history` command.

If you reload the Firepower Threat Defense device, the memory allocation returns to the default.

The amount of memory allocated will be at most 150 KB, but never more than 50% of free memory. Optionally, you can specify the memory size manually.

**Examples**

The following example increases the memory size for block diagnostics:

```
> blocks queue history enable
```

The following example increases the memory size to 3000 bytes:

```
> blocks queue history enable 3000
```

The following example attempts to increase the memory size to 3000 bytes, but the value is more than the available free memory:

```
> blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

The following example increases the memory size to 3000 bytes, but the value is more than 50% of the free memory:

```
> blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear blocks</td>
<td>Clears the system buffer statistics.</td>
</tr>
<tr>
<td>show blocks</td>
<td>Shows the system buffer usage.</td>
</tr>
</tbody>
</table>
**capture**

To enable packet capture capabilities for packet sniffing and network fault isolation, use the `capture` command. To disable packet capture capabilities, use the no form of this command.

Capture network traffic:

```
capture capture_name [type {asp-drop [all | drop-code] | raw-data | isakmp [ikev1 | ikev2] | inline-tag [tag]}] [interface {interface_name | data-plane | management-plane | cplane}] [buffer buf_size] [file-size file_size] [ethernet-type type] [headers-only] [packet-length bytes] [circular-buffer] [trace [trace-count number]] [match protocol {host source_ip | source_ip mask | any4 | any6} [operator src_port] {host dest_ip | dest_ip mask | any4 | any6} [operator dest_port]]
```

Capture cluster control-link traffic:

```
capture capture_name type lacp interface interface_id [buffer buf_size] [packet-length bytes] [circular-buffer] [real-time [dump] [detail]]
```

Capture packets cluster-wide:

```
capture capture_name interface cluster [buffer buf_size] [ethernet-type type] [packet-length bytes] [circular-buffer] [trace [trace-count number]] [real-time [dump] [detail]] [match protocol {host source_ip | source_ip mask | any4 | any6} [operator src_port] {host dest_ip | dest_ip mask | any4 | any6} [operator dest_port]]
```

Capture packets cluster-wide:

```
capture capture_name arguments
```

Stop or remove the packet capture:

```
no capture capture_name [arguments]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any4</td>
<td>Specifies any IPv4 address instead of a single IP address and mask.</td>
</tr>
<tr>
<td>any6</td>
<td>Specifies any IPv6 address instead of a single IP address and mask.</td>
</tr>
<tr>
<td>all</td>
<td>Captures all packets dropped by the accelerated security path.</td>
</tr>
<tr>
<td>asp-drop drop-code</td>
<td>(Optional) Captures packets dropped by the accelerated security path. The drop-code specifies the type of traffic that is dropped by the accelerated security path. See the CLI help for a list of drop codes. You can enter this keyword with the <code>packet-length</code>, <code>circular-buffer</code>, and <code>buffer</code> keywords, but not with the <code>interface</code> or <code>ethernet-type</code> keyword. In a cluster, dropped forwarded data packets from one unit to another are also captured.</td>
</tr>
<tr>
<td>buffer buf_size</td>
<td>(Optional) Defines the buffer size used to store the packet in bytes. Once the byte buffer is full, packet capture stops. When used in a cluster, this is the per-unit size, not the sum of all units. The maximum buffer size supported is 32 MB. The buffer size and file size options are mutually exclusive.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>capture_name</td>
<td>Specifies the name of the packet capture. Use the same name on multiple capture statements to capture multiple types of traffic. When you view the capture configuration using the show capture command, all options are combined on one line.</td>
</tr>
<tr>
<td>data-plane</td>
<td>Specifies the captured packets on the dataplane interface.</td>
</tr>
<tr>
<td>management-plane</td>
<td>Specifies the captured packets on the management interface.</td>
</tr>
<tr>
<td>circular-buffer</td>
<td>(Optional) Overwrites the buffer, starting from the beginning, when the buffer is full.</td>
</tr>
<tr>
<td>ethernet-type</td>
<td>(Optional) Selects an Ethernet type to capture. Supported Ethernet types include 8021Q, ARP, IP, IP6, IPX, LACP, PPPOED, PPPOES, RARP, and VLAN. An exception occurs with the 802.1Q or VLAN type. The 802.1Q tag is automatically skipped and the inner Ethernet type is used for matching.</td>
</tr>
<tr>
<td>file-size</td>
<td>(Optional) file-size specifies capturing packets to a file on disk. The file-size specifies the size of capture file from 32 MB to 10 GB. The capture file will be created in flash memory (disk0:/) with the name capture_name.pcap.</td>
</tr>
<tr>
<td></td>
<td>When the file-size is configured, the hard disk memory (file) is used to write the captured data in the capture buffer. The captured data gets stored in the disk based on the filename. The buffer size and file size options are mutually exclusive.</td>
</tr>
<tr>
<td>headers-only</td>
<td>(Optional) Selects Layer 2 and Layer 3/4 headers of packet to capture without data.</td>
</tr>
<tr>
<td>host</td>
<td>Specifies the single IP address of the host to or from which the packet is being sent.</td>
</tr>
<tr>
<td>inline-tag</td>
<td>Specifies a tag for a particular SGT value or leaves it unspecified to capture a tagged packet with any SGT value.</td>
</tr>
<tr>
<td>interface</td>
<td>Sets the name of the interface on which to use packet capture. You must configure an interface for any packets to be captured except for type asp-drop. You can configure multiple interfaces using multiple capture commands with the same name. To capture packets on the management plane, you can use the interface keyword with asa_mgmt_plane as the interface name. You can specify cluster as the interface name to capture the traffic on the cluster control link interface. If the type lacp capture is configured, the interface name is the physical name.</td>
</tr>
<tr>
<td>ikev1, ikev2</td>
<td>Captures only IKEv1 or IKEv2 protocol information.</td>
</tr>
<tr>
<td>isakmp</td>
<td>(Optional) Captures ISAKMP traffic for VPN connections. The ISAKMP subsystem does not have access to the upper layer protocols. The capture is a pseudo capture, with the physical, IP, and UDP layers combined together to satisfy a PCAP parser. The peer addresses are obtained from the SA exchange and are stored in the IP layer.</td>
</tr>
<tr>
<td>lacp</td>
<td>(Optional) Captures LACP traffic. If configured, the interface name is the physical interface name.</td>
</tr>
</tbody>
</table>
mask

The subnet mask for the IP address, for example, 255.255.255.0 for a Class C mask.

match protocol

Specifies the packets that match the five-tuple to allow filtering of those packets to be captured. You can use this keyword up to three times on one line.

operator src_port, dest_port

(Optional) Matches the port numbers used by the source or destination. The permitted operators are as follows:

• lt—less than
• gt—greater than
• eq—equal to
• neq—not equal to
• range—range

packet-length bytes

(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.

raw-data

(Optional) Captures inbound and outbound packets on one or more interfaces.

trace trace_count

(Optional) Captures packet trace information, and the number of packets to capture. This option is used with an access list to insert trace packets into the data path to determine whether or not the packet has been processed as expected.

type

(Optional) Specifies the type of data captured.

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>The defaults are as follows:</td>
</tr>
<tr>
<td>• The default type is raw-data.</td>
</tr>
<tr>
<td>• The default buffer size is 512 KB.</td>
</tr>
<tr>
<td>• The default Ethernet type is IP packets.</td>
</tr>
<tr>
<td>• The default packet-length is 1518 bytes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>6.2.1</td>
<td>This command was updated to store the contents of all the active captures to files on flash or disks at the time of box crash.</td>
</tr>
<tr>
<td></td>
<td>6.2.3</td>
<td>The options asa_mgmt_plane and asa_dataplane were renamed to management-plane and data-plane respectively.</td>
</tr>
<tr>
<td></td>
<td>6.2.3.x</td>
<td>The options any4 and any6 were introduced to capture IPv4 and IPv6 network traffic respectively.</td>
</tr>
<tr>
<td></td>
<td>6.3</td>
<td>The option [file-size file-size] allows you to capture file size in MB (32-10000).</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

Capturing packets is useful when troubleshooting connectivity problems or monitoring suspicious activity. You can create multiple captures. The `capture` command is not saved to the running configuration, and is not copied to the standby unit during high availability.

The Firepower Threat Defense device is capable of tracking all IP traffic that flows across it and of capturing all the IP traffic that is destined to it, including all the management traffic (such as SSH and Telnet traffic).

The Firepower Threat Defense architecture consists of three different sets of processors for packet processing; this architecture poses certain restrictions on the capability of the capture feature. Typically most of the packet forwarding functionality in the Firepower Threat Defense device is handled by the two front-end network processors, and packets are sent to the control-plane general-purpose processor only if they need application inspection. The packets are sent to the session management path network processor only if there is a session miss in the accelerated path processor.

Because all the packets that are forwarded or dropped by the Firepower Threat Defense device hits the two front-end network processors, the packet capture feature is implemented in these network processors. So all the packets that hit the Firepower Threat Defense device can be captured by these front end processors, if an appropriate capture is configured for those traffic interfaces. On the ingress side, the packets are captured the moment the packet hits the interfaces, and on the egress side the packets are captured just before they are sent out on the wire.

To save the captured data, packet capture automatically writes captured data to the physical storage on the fly, without having to use the `copy` command. The capture size is supported up to 10 GB. Captures larger than 100 MB are automatically compressed.

**Save the Capture**

The contents of any active capture on Firepower Threat Defense device are saved when the box crashes. When you activate captures as part of the troubleshooting process, you must note the following points:

- The size of capture buffer to use and if there is enough space on flash/disk.
- The capture buffer should be marked as circular for all the use cases, so that captured packets are the most recent before crash.

The name of the file for saving contents of an active capture is in the format of:

```
/ <context_name>.<capture_name>.pcap
```

The `context_name` indicates the name of the user context in which capture is activated in the multi-context mode. For the single context mode, the `context_name` is not applicable.

The `capture_name` indicates the name of the capture that is activated.

The capture save happens before the console or crash dump. This increases the crash downtime by about 5 seconds for a 33 MB capture buffer. The risk of a nested crash is minimal because copying the captured contents to a file is a simple process.

**View the Capture**

To view the packet capture, use the `show capture name` command. To save the capture to a file, use the `copy capture` command. Use the `https://FTP-ip-address/admin/capture/capture_name/[pcap]` command to see the packet capture information with a web browser. If you specify the `pcap` keyword, then a libpcap-format file is downloaded to the web browser and can be saved using the web browser. (A libcap file can be viewed with TCPDUMP or Ethereal.)
If you copy the buffer contents to a TFTP server in ASCII format, you will see only the headers, not the details and hexadecimal dump of the packets. To see the details and hexadecimal dump, you need to transfer the buffer in PCAP format and read it with TCPDUMP or Ethereal.

Delete the Capture

Entering `no capture` without any keywords deletes the capture. To preserve the capture, specify the `interface` keyword; the capture is detached from the specified interface, and the capture is preserved.

Clustering

You can precede the `capture` command with `cluster exec` to issue the `capture` command on one unit and run the command in all the other units at the same time. After you have performed cluster-wide capture, to copy the same capture file from all units in the cluster at the same time to a TFTP server, enter the `cluster exec copy` command on the master unit.

```
cluster exec capture capture_name arguments
```

```
cluster exec copy /pcap capture: cap_name tftp://location/path/filename.pcap
```

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as `filename_A.pcap`, `filename_B.pcap`, and so on. In this example, A and B are cluster unit names.

---

**Note**

A different destination name is generated if you add the unit name at the end of the filename.

---

Limitations

The following are some of the limitations of the capture feature. Most of the limitations are caused by the distributed nature of the Firepower Threat Defense architecture and by the hardware accelerators that are being used in the Firepower Threat Defense device.

- For inline SGT tagged packets, captured packets contain an additional CMD header that your PCAP viewer might not understand.
- If there is no ingress interface and therefore no global interface, packets sent on the backplane are treated as control packets. These packets bypass the access list check and are always captured.
- The `show capture` command shows the correct reason when capturing a specific asp-drop. However, the `show capture` command does not show the correct reason when capturing all asp-drops.

The packet capture feature with the file-size option has the following limitations:

- Applicable only for Firepower 4000 and Firepower 9000 series.
- For existing capture, you cannot add the file size option.
- The `copy` command is not supported.
- Real-time, trace, linear, and circular buffer are not supported.
- If the number of captures with the file size option is increased, the performance of the system will be reduced.
- If the system load is high, it leads to packet capture data loss.
Examples
To capture a packet, enter the following command:

> capture captest interface inside
> capture captest interface outside

On a web browser, you can view the content of the capture command that was issued, named “capttest,” at the following location:

https://171.69.38.95/admin/capture/captest

To download a libpcap file (that web browsers use) to a local machine, enter the following command:

https://171.69.38.95/capture/http/pcap

The following example shows how to capture a packet in the single-mode when the Firepower Threat Defense Device crashes:

> capture 789 interface inside

The contents of capture ‘789’ is saved as 789.pcap file.

The following example shows how to capture a packet in the multi-mode when the Firepower Threat Defense device crashes:

> capture 624 interface inside

The contents of capture ‘624’ in admin context is saved as admin.624.pcap file.

The following example shows how to capture ARP packets:

> capture arp ethernet-type arp interface outside

Capture for Clustering
To enable capture on all units in the cluster, you can add the cluster exec keywords in front of each of these commands.

The following example shows how to create an LACP capture for the clustering environment:

> capture lacp type lacp interface gigabitEthernet0/0

The following example shows how to create a capture for control path packets in the clustering link:

> capture cp interface cluster match udp any eq 49495 any
> capture cp interface cluster match udp any eq 49495
The following example shows how to capture data path traffic through the cluster:

```plaintext
> capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
> capture abc interface inside match dup host 1.1.1.1 any
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clear capture</td>
<td>Clears the capture buffer.</td>
</tr>
<tr>
<td></td>
<td>copy capture</td>
<td>Copies a capture file to a server.</td>
</tr>
<tr>
<td></td>
<td>show capture</td>
<td>Displays the capture configuration when no options are specified.</td>
</tr>
</tbody>
</table>

Cisco Firepower Threat Defense Command Reference
To intercept and capture packets passing through a Firepower Threat Defense interface, use the `capture-traffic` command. You can capture traffic on a specified Firepower Threat Defense domain that matches the integer expression from the list of options presented, either the management interface (br1) or traffic interfaces.

You are prompted for the domain and TCP dump options.

**Syntax Description**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Specifies the domain where traffic is captured:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>br1, captures traffic from the management interface</td>
</tr>
<tr>
<td>1</td>
<td>Router, captures traffic from the configured data interfaces</td>
</tr>
</tbody>
</table>

**-A**

Prints each packet (minus its link level header) in ASCII. Handy for capturing web pages.

**-B**

Sets the operating system capture buffer size to buffer_size.

**-c**

Exits after receiving count packets.

**-C**

Before writing a raw packet to a savefile, checks whether the file is currently larger than file_size and, if so, close the current savefile and open a new one. Savefiles after the first savefile will have the name specified with the -w flag, with a number after it, starting at 1 and continuing upward. The units of file_size are millions of bytes (1,000,000 bytes, not 1,048,576 bytes).

**-d**

Dumps the compiled packet-matching code in a human readable form to standard output and stop.

**-dd**

Dumps packet-matching code as a C program fragment.

**-ddd**

Dumps packet-matching code as decimal numbers (preceded with a count).

**-D**

Prints the list of the network interfaces available on the system and on which tcpdump can capture packets. For each network interface, a number and an interface name, possibly followed by a text description of the interface, is printed. The interface name or the number can be supplied to the -i flag to specify an interface on which to capture.

This can be useful on systems that do not have a command to list them (Windows systems, or UNIX systems lacking ifconfig -a); the number can be useful on Windows 2000 and later systems, where the interface name is a somewhat complex string.

The -D flag will not be supported if tcpdump was built with an older version of libpcap that lacks the pcap_findalldevs() function.

**-e**

Prints the link-level header on each dump line.

**-E**

Uses spi@ipaddr algo:secret for decrypting IPsec ESP packets that are addressed to addr and contain Security Parameter Index value spi. This combination may be repeated with comma or newline separation.
| **-f** | Prints ‘foreign’ IPv4 addresses numerically rather than symbolically (this option is intended to get around serious brain damage in Sun's NIS server usually it hangs forever translating non-local internet numbers).

The test for ‘foreign’ IPv4 addresses is done using the IPv4 address and netmask of the interface on which capture is being done.

If that address or netmask are not available, available, either because the interface on which capture is being done has no address or netmask or because the capture is being done on the Linux 'any' interface, which can capture on more than one interface, this option will not work correctly. |
| **-F** | Uses file as input for the filter expression. An additional expression given on the command line is ignored. |
| **-G** | If specified, rotates the dump file specified with the -w option every rotate_seconds seconds.

Save files will have the name specified by -w which should include a time format as defined by strftime(3). If no time format is specified, each new file will overwrite the previous.

If used in conjunction with the -C option, filenames will take the form of ‘file<count>'). |
| **-I** | Puts the interface in ‘monitor mode’; this is supported only on IEEE 802.11 Wi-Fi interfaces, and supported only on some operating systems. |
| **-K** | Does not attempt to verify TCP checksums.

This is useful for interfaces that perform the TCP checksum calculation in hardware; otherwise, all outgoing TCP checksums will be flagged as bad. |
| **-l** | Makes stdout line buffered. Useful if you want to see the data while capturing it.

Example, “tcpdump -l | tee dat” or “tcpdump -l > dat & tail -f dat”.
| **-L** | Lists the known data link types for the interface and exit. |
| **-m** | Loads SMI MIB module definitions from file module.

This option can be used several times to load several MIB modules into tcpdump. |
| **-M** | Uses secret as a shared secret for validating the digests found in TCP segments with the TCP-MD5 option (RFC 2385), if present. |
| **-n** | Does not convert addresses (i.e., host addresses, port numbers, etc.) to names. |
| **-N** | Does not print domain name qualification of host names.

Example, if you give this flag then tcpdump will print “nic” instead of “nic.ddn.mil”. |
| **-O** | Does not run the packet-matching code optimizer. This is useful only if you suspect a bug in the optimizer. |
| **-p** | Does not put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, `-p' cannot be used as an abbreviation for ’ether host {local-hw-addr} or ether broadcast'.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-q</td>
<td>Quick output. Prints less protocol information so output lines are shorter.</td>
</tr>
<tr>
<td>-R</td>
<td>Assumes ESP/AH packets to be based on old specification (RFC1825 to RFC1829). If specified, tcpdump will not print replay prevention field. Because there is no protocol version field in ESP/AH specification, tcpdump cannot deduce the version of ESP/AH protocol.</td>
</tr>
<tr>
<td>-r</td>
<td>Reads packets from file (which was created with the -w option). Standard input is used if file is “-”.</td>
</tr>
<tr>
<td>-S</td>
<td>Prints absolute, rather than relative, TCP sequence numbers.</td>
</tr>
<tr>
<td>-s</td>
<td>Snarf snaplen bytes of data from each packet rather than the default of 68 (with SunOS’s NIT, the minimum is actually 96). 68 bytes is adequate for IP, ICMP, TCP, and UDP but may truncate protocol information from name server and NFS packets (see below). Packets truncated because of a limited snapshot are indicated in the output with “[/proto]”, where proto is the name of the protocol level at which the truncation has occurred. Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. You should limit snaplen to the smallest number that will capture the protocol information you're interested in. Setting snaplen to 0 means use the required length to catch whole packets.</td>
</tr>
<tr>
<td>-T</td>
<td>Forces packets selected by ‘expression’ to be interpreted the specified type. Currently known types are adv (Ad-hoc On-demand Distance Vector protocol), cnfp (Cisco NetFlow protocol), rpc (Remote Procedure Call), rtp (Real-Time Applications protocol), rtcp (Real-Time Applications control protocol), snmp (Simple Network Management Protocol), tftp (Trivial File Transfer Protocol), vat (Visual Audio Tool), and wb (distributed White Board).</td>
</tr>
<tr>
<td>-t</td>
<td>Does not print a timestamp on each dump line.</td>
</tr>
<tr>
<td>-tt</td>
<td>Prints an unformatted timestamp on each dump line.</td>
</tr>
<tr>
<td>-ttt</td>
<td>Prints a delta (micro-second resolution) between current and previous line on each dump line.</td>
</tr>
<tr>
<td>-tttt</td>
<td>Prints a timestamp in default format proceeded by date on each dump line.</td>
</tr>
<tr>
<td>-ttttt</td>
<td>Prints a delta (micro-second resolution) between current and first line on each dump line.</td>
</tr>
<tr>
<td>-u</td>
<td>Prints undecoded NFS handles.</td>
</tr>
<tr>
<td>-U</td>
<td>Makes output saved via the -w option “packet-buffered”; i.e., as each packet is saved, it will be written to the output file, rather than being written only when the output buffer fills. The -U flag will not be supported if tcpdump was built with an older version of libpcap that lacks the pcap_dump_flush() function.</td>
</tr>
</tbody>
</table>
When parsing and printing, produces (slightly more) verbose output. For example, the
time to live, identification, total length and options in an IP packet are printed. Also
enables additional packet integrity checks such as verifying the IP and ICMP header
checksum.

When writing to a file with the -w option, report, every 10 seconds, the number of
packets captured.

-vv
Even more verbose output. For example, additional fields are printed from NFS reply
packets, and SMB packets are fully decoded.

-vvv
Even more verbose output. For example, telnet SB... SE options are printed in full.
With -X Telnet options are printed in hex as well.

-w
Write the raw packets to file rather than parsing and printing them out. They can later
be printed with the -r option. Standard output is used if file is “-”.

-W
Used in conjunction with the -C option, this will limit the number of files created to
the specified number, and begin over writing files from the beginning, thus creating a
‘rotating’ buffer. In addition, it will name the files with enough leading 0s to support
the maximum number of files, allowing them to sort correctly.

-x
When parsing and printing, in addition to printing the headers of each packet, prints
the data of each packet (minus its link level header) in hex. The smaller of the entire
packet or snaplen bytes will be printed. Note that this is the entire link-layer packet,
so for link layers that pad (e.g. Ethernet), the padding bytes will also be printed when
the higher layer packet is shorter than the required padding.

-xx
When parsing and printing, in addition to printing the headers of each packet, prints
the data of each packet, including its link level header, in hex.

-X
When parsing and printing, in addition to printing the headers of each packet, print
the data of each packet (minus its link level header) in hex and ASCII.
This is very handy for analyzing new protocols.

-XX
When parsing and printing, in addition to printing the headers of each packet, prints
the data of each packet, including its link level header, in hex and ASCII.

-y
Sets the data link type to use while capturing packets to datalinktype.

-Z
Drops privileges (if root) and changes user ID to user and the group ID to the primary
group of user.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

By default the capture-traffic command produces one line of text per every packet it intercepts. Each line
includes: a time stamp; the protocol name; the source and destination addresses (for IP packets, these are IP
addresses; for other protocols, capture-traffic does not print any identifiers unless explicitly asked to do so
(see the -e command line description)); and information including TCP sequence numbers, flags, ARP/ICMP
commands, and so on.
Note

The pcap file (output of the `capture-traffic` or `debug daq` command) displays untranslated details of the packet that was received; the **Connection Events** list (Firepower Management Center) displays translated packet details that are actually applied with the policies.

To stop the capture, type Control + C. If you use `-w outputfile` option, the packet capture will be saved with that file name in `/var/common/`. Otherwise it is written to the display.

Examples

The following example shows how to capture traffic from the management interface:

```
> capture-traffic
Please choose domain to capture traffic from:
  0 - br1
  1 - Router
Selection? 0
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
  -v
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show traffic</td>
<td>Displays traffic statistics.</td>
</tr>
<tr>
<td>show interface</td>
<td>Displays interface status information.</td>
</tr>
</tbody>
</table>
# clear aaa-server statistics

To reset statistics for AAA servers, use the `clear aaa-server statistics` command.

```plaintext
clear aaa-server statistics  [LOCAL  |  groupname  [host  hostname]  |  protocol  protocol]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>groupname</code></td>
<td>(Optional) Clears statistics for servers in a group.</td>
</tr>
<tr>
<td><code>host hostname</code></td>
<td>(Optional) Clears statistics for a particular server in the group.</td>
</tr>
<tr>
<td><code>LOCAL</code></td>
<td>(Optional) Clears statistics for the LOCAL user database.</td>
</tr>
<tr>
<td><code>protocol protocol</code></td>
<td>(Optional) Clears statistics for servers of the specified protocol. Enter ? to see the available protocols.</td>
</tr>
</tbody>
</table>

## Command Default

Removes all AAA server statistics across all groups.

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Examples

The following example shows how to reset the AAA statistics for all server groups:

> `clear aaa-server statistics`

The following example shows how to reset the AAA statistics for an entire server group:

> `clear aaa-server statistics svrgrp1`

The following example shows how to reset the AAA statistics for a specific server in a group:

> `clear aaa-server statistics svrgrp1 host 10.2.3.4`

## Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aaa-server</td>
<td>Displays AAA server statistics</td>
</tr>
</tbody>
</table>
clear access-list

To clear an access-list counter, use the clear access-list command.

```
clear access-list  id
```

**Syntax Description**

| id | Name of an access list. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you enter the `clear access-list` command, you must specify the `id` of an access list to clear the counters. Use the `show access-list` command for a list of ACLs.

**Examples**

The following example shows how to clear a specific access list counter:

```
> clear access-list inbound
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show access-list</code></td>
<td>Displays the access list entries by number.</td>
</tr>
<tr>
<td><code>show running-config access-list</code></td>
<td>Displays the access list configuration that is running on the adaptive security appliance.</td>
</tr>
</tbody>
</table>
clear arp

To clear dynamic ARP entries or ARP statistics, use the **clear arp** command.

```
clear arp [statistics | interface_name]
```

**Syntax Description**
- **statistics**: Clears ARP statistics.
- **interface_name**: Clears statistics for the specified interface.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears all ARP statistics:

```
> clear arp statistics
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show arp statistics</td>
<td>Shows ARP statistics.</td>
</tr>
<tr>
<td>show running-config arp</td>
<td>Shows the current configuration of the ARP timeout.</td>
</tr>
</tbody>
</table>
clear asp

To clear accelerated security path (ASP) statistics, use the `clear asp` command.

```
```

**Syntax Description**

- `access-list acl_name` (Optional) Clears the hit counters only for a specified access list.
- `arp` (Optional) Clears the hits counters in ASP ARP tables only.
- `classify` (Optional) Clears the hits counters in ASP classify tables only.
- `cluster counter` Clears cluster counters.
- `counters` Clears the data-path inspection Snort counters.
- `dispatch` Clears dispatch statistics.
- `event` Clears data-path to control-plane event statistics.
- `filter` (Optional) Clears the hits counters in ASP filter tables only.
- `flow` (Optional) Clears the dropped flow statistics.
- `frame` (Optional) Clears the dropped frame/packet statistics.
- `inspect-dp egress-optimization` (Optional) Clears egress optimization statistics.
- `inspect-dp snort` Clears data-path inspection Snort statistics.
- `instance number` (Optional) Clears the counters by instance ID.
- `load-balance history` Clears the history of ASP load balancing per packet and reset the number of times an automatic switch occurred.
- `overhead` Clears all ASP multiprocessor overhead statistics.
- `packet-profile` Clears packet profile statistics.
- `queue number` (Optional) Clears the counters by instance ID and queue ID.
- `queue-exhaustion` Clears the data-path inspection Snort queue snapshot.
- `snapshot number` (Optional) Clears the queue exhaustion by snapshot ID.
- `table` Clears the hit counters in ASP ARP tables and ASP classify tables.
clear asp

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.4</td>
<td>The <code>clear asp inspect-dp egress-optimization</code> command was introduced.</td>
</tr>
<tr>
<td>6.5</td>
<td>The <code>packet-profile</code> keyword was added.</td>
</tr>
</tbody>
</table>

Examples

The following example clears all dispatch statistics:

```plaintext
> clear asp dispatch
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show asp</td>
<td>Shows ASP statistics.</td>
</tr>
</tbody>
</table>
clear bfd

To clear all bi-directional forwarding detection (BFD) counters, use the **clear bfd counters** command.

```plaintext
clear bfd counters [ld local_discr | interface_name | ipv4 ip_address | ipv6 ip_address]
```

**Syntax Description**

- **ld local_discr** (Optional) Clears BFD counters for the specified local discriminator, 1 - 4294967295.
- **interface_name** (Optional) Clears BFD counters for the specified interface.
- **ipv4 ip_address** (Optional) Clears BFD counters for the specified neighbor IPv4 address.
- **ipv6 ip_address** (Optional) Clears BFD counters for the specified neighbor IPv6 address.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears all BFD counters:

```plaintext
> clear bfd counters
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show bfd</td>
<td>Shows BFD protocol information, including packets dropped, neighbors, and map entries.</td>
</tr>
</tbody>
</table>
clear bgp

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use the `clear bgp` command.

```
clear bgp { [* | external ] [ ipv4 unicast [ as_number | neighbor_address | table-map ] ] | ipv6 unicast [ as_number | neighbor_address ] [ soft [ in | out ] | as_number [ soft ] [ in | out ] | neighbor_address [ soft ] [ in | out ] | table-map ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Specifies that all current BGP sessions will be reset.</td>
</tr>
<tr>
<td>as_number</td>
<td>(Optional) Number of the autonomous system in which all BGP peer sessions will be reset.</td>
</tr>
<tr>
<td>external</td>
<td>Specifies that all external BGP sessions will be reset.</td>
</tr>
<tr>
<td>in</td>
<td>(Optional) Initiates inbound reconfiguration. If neither the <code>in</code> nor <code>out</code> keywords are specified, both inbound and outbound sessions are reset.</td>
</tr>
<tr>
<td>ipv4 unicast</td>
<td>Resets BGP connections using hard or soft reconfiguration for IPv4 address family sessions.</td>
</tr>
<tr>
<td>ipv6 unicast</td>
<td>Resets BGP connections using hard or soft reconfiguration for IPv6 address family sessions.</td>
</tr>
<tr>
<td>neighbor_address</td>
<td>(Optional) Specifies that only the identified BGP neighbor will be reset. The value for this argument can be an IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>out</td>
<td>(Optional) Initiates inbound or outbound reconfiguration. If neither the <code>in</code> nor <code>out</code> keywords are specified, both inbound and outbound sessions are reset.</td>
</tr>
<tr>
<td>soft</td>
<td>(Optional) Clears slow-peer status forcefully, and moves it to original update group.</td>
</tr>
<tr>
<td>table-map</td>
<td>Clears table-map configuration information in BGP routing tables. This command can be used to clear traffic-index information configured with the BGP Policy Accounting feature.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `clear bgp` command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply a new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.
Examples

In the following example, all the BGP sessions are reset:

```
> clear bgp *
```

In the following example, a soft reconfiguration is initiated for the inbound session with the neighbor 10.100.0.1, and the outbound session is unaffected:

```
> clear bgp 10.100.0.1 soft in
```

In the following example, the route refresh capability is enabled on the BGP neighbor routers, a soft reconfiguration is initiated for the inbound session with the neighbor 172.16.10.2, and the outbound session is unaffected:

```
> clear bgp 172.16.10.2 in
```

In the following example, a hard reset is initiated for sessions with all routers in the autonomous system numbered 35700:

```
> clear bgp 35700
```

In the following example, a soft reconfiguration is configured for all inbound eBGP peering sessions:

```
> clear bgp external soft in
```

In the following example, all outbound address family IPv4 multicast eBGP peering sessions are cleared:

```
> clear bgp external ipv4 multicast out
```

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in IPv4 unicast address family sessions in autonomous system 65400, and the outbound session is unaffected:

```
> clear bgp ipv4 unicast 65400 soft in
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation:

```
> clear bgp ipv4 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation:

```
> clear bgp ipv4 unicast 1.2
```
The following example clears the table map for IPv4 unicast peering sessions:

> clear bgp ipv4 unicast table-map
clear blocks

To reset the packet buffer counters such as the exhaustion condition and history information, use the `clear blocks` command.

```
clear blocks [exhaustion {history | snapshot} | export-failed | queue {history [core-local [number]]}]]
```

**Syntax Description**
- `core-local [number]` (Optional) Clears system buffers queued by application for all cores, or if you specify the core number, a specific core.
- `exhaustion` (Optional) Clears the exhaustion condition.
- `export-failed` (Optional) Clears the export failed counters.
- `history` (Optional) Clears the history.
- `queue` (Optional) Clears queued blocks.
- `snapshot` (Optional) Clears the snapshot information.

**Command History**
```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**
Resets the low watermark counters to the current available blocks in each pool. Additionally, this command clears the history information stored during the last buffer allocation failure.

**Examples**
The following example clears the blocks:

```
> clear blocks
```

**Related Commands**
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blocks</td>
<td>Increases the memory assigned to block diagnostics.</td>
</tr>
<tr>
<td>show blocks</td>
<td>Shows the system buffer utilization.</td>
</tr>
</tbody>
</table>
clear capture

To clear the capture buffer, use the `clear capture` command.

```
clear capture (/all | capture_name)
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/all</code></td>
<td>Clears packets on all interfaces.</td>
</tr>
<tr>
<td><code>capture_name</code></td>
<td>Specifies the name of the packet capture.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to clear the capture buffer for the capture buffer “example.”

```
> clear capture example
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>capture</code></td>
<td>Enables packet capture capabilities for packet sniffing and network fault isolation.</td>
</tr>
<tr>
<td><code>show capture</code></td>
<td>Displays the capture configuration when no options are specified.</td>
</tr>
</tbody>
</table>
To clear Connectionless-mode Network Protocol (CLNP) information, use the `clear clns` command.

```
clear clns { is-neighbors | neighbors | traffic }
```

### Syntax Description
- `is-neighbors`: Clears intermediate-system neighbor routes.
- `neighbors`: Clears all CLNS neighbor routes.
- `traffic`: Clears CLNS protocol statistics.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to clear all CLNS neighbor routes:

```
> clear clns neighbors
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show clns</td>
<td>Displays Connectionless-mode Network Protocol (CLNP) network information.</td>
</tr>
</tbody>
</table>
clear cluster info

To clear cluster statistics, use the `clear cluster info` command.

```
clear cluster info { flow-mobility counters | health details | trace | transport }
```

**Syntax Description**
- **flow-mobility counters**: Clears the cluster flow-mobility counters.
- **health details**: Clears cluster health information.
- **trace**: Clears cluster event trace information.
- **transport**: Clears cluster transport statistics.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To view cluster statistics, use the `show cluster info` command.

**Examples**

The following example clears cluster event trace information:

```
> clear cluster info trace
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cluster info</td>
<td>Shows cluster statistics.</td>
</tr>
</tbody>
</table>
clear configure key chain

To remove the key chains that are configured, use the **clear configure key chain** command.

**clear configure key chain**

**key-chain-name**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **clear configure key chain** command to remove the configured key chain.

**Examples**

The following example shows how to remove the configured key chain.

```
> clear configure key chain CHAIN1
>```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key chain</td>
<td>Configure the key chains for ospfv2 authentication.</td>
</tr>
<tr>
<td>show key chain</td>
<td>Displays the configured key chains.</td>
</tr>
<tr>
<td>show running key chain</td>
<td>Displays the key chain details that is currently active.</td>
</tr>
</tbody>
</table>
clear conn

To clear a specific connection or multiple connections, use the **clear conn** command.

```
clear conn { all | protocol { tcp | udp | sctp } | address ip [-ip] [netmask mask] | port port [-port] | inline-set name | security-group { name | tag } attribute | user [domainNickname\user_name | user-group [domainNickname\user_group_name | zone [zone_name] }
```

**Syntax Description**

- **address ip[-ip]**
  Clears connections with the specified source or destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: 10.1.1.1-10.1.1.5

- **all**
  Clears all connections, including to-the-box connections. Without the all keyword, only through-the-box connections are cleared.

- **inline-set name**
  Clears connections that match the specified inline set.

- **netmask mask**
  (Optional) Specifies a subnet mask for use with the given IP address.

- **port port[-port]**
  Clears connections with the specified source or destination port. To specify a range, separate the port numbers with a dash (-). For example: 1000-2000

- **protocol { tcp | udp | sctp }**
  Clears connections with the specified protocol.

- **security-group { name | tag } attribute**
  Clears connections that belong to the specified security group attribute.

- **user [domainNickname\user_name**
  Clears connections that belong to the specified user. When you do not include the *domainNickname* argument, the system clears connections for the user in the default domain.

- **user-group [domainNickname\user_group_name**
  Clears connections that belong to the specified user group. When you do not include the *domainNickname* argument, the system clears connections for the user group in the default domain.

- **zone [zone_name]**
  Clears connections that belong to a security zone.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you make security policy changes to the configuration, all new connections use the new security policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy using the **clear conn** command. You can alternatively use the **clear local-host** command to clear connections per host, or the **clear xlate** command for connections that use dynamic NAT.

When the device creates a pinhole to allow secondary connections, this is shown as an incomplete connection in the **show conn** command output. To clear this incomplete connection, use the **clear conn** command.
This command does not clear connections to the Management interface; it can only clear management connections to a data interface or the Diagnostic interface.

Examples

The following example shows how to view all connections and then clear the management connection from 10.10.10.108:

```
> show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags UOB
> clear conn address 10.10.10.108
```
clear console-output

To remove the currently captured console output, use the clear console-output command.

```
clear console-output
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to remove the currently captured console output:

```
> clear console-output
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show console-output</td>
<td>Displays the captured console output.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the idle timeout for a console connection to the device.</td>
</tr>
<tr>
<td>console timeout</td>
<td></td>
</tr>
</tbody>
</table>
clear counters

To clear the protocol stack counters, use the `clear counters` command.

```
clear counters [all | summary | top n] [detail] [protocol protocol_name [counter_name]]
[threshold n]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>(Optional) Clears all filter details.</td>
</tr>
<tr>
<td><code>counter_name</code></td>
<td>(Optional) Specifies a counter by name. Use the <code>show counters protocol</code> command to see available counter names.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Clears detailed counters information.</td>
</tr>
<tr>
<td><code>protocol protocol_name</code></td>
<td>(Optional) Clears the counters for the specified protocol.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>(Optional) Clears the counter summary.</td>
</tr>
<tr>
<td><code>threshold n</code></td>
<td>(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.</td>
</tr>
<tr>
<td><code>top n</code></td>
<td>(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.</td>
</tr>
</tbody>
</table>

**Command Default**

The `clear counters summary detail` command is the default.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the protocol stack counters:

```
> clear counters
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show counters</td>
<td>Displays the protocol stack counters.</td>
</tr>
</tbody>
</table>
clear cpu profile

To clear the CPU profiling statistics, use the clear cpu command.

clear cpu profile

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to delete the crash file:

> clear cpu profile

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cpu</td>
<td>Displays information about the CPU.</td>
</tr>
<tr>
<td>show cpu profile</td>
<td>Displays CPU profiling data.</td>
</tr>
</tbody>
</table>
clear crashinfo

To delete the contents of the crash file in flash memory, use the **clear crashinfo** command.

```
clear crashinfo  [ module  { 0 | 1 } ]
```

**Syntax Description**

| module {0 | 1} | (Optional) Clears the crash file for a module in slot 0 or 1. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to delete the crash file:

```
> clear crashinfo
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crashinfo force</td>
<td>Forces a crash of the system.</td>
</tr>
<tr>
<td>crashinfo test</td>
<td>Tests the ability of the system to save crash information to a file in flash memory.</td>
</tr>
<tr>
<td>show crashinfo</td>
<td>Displays the contents of the crash file stored in flash memory.</td>
</tr>
</tbody>
</table>
clear crypto accelerator statistics

To clear the global and accelerator-specific statistics from the crypto accelerator MIB, use the `clear crypto accelerator statistics` command.

**clear crypto accelerator statistics**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> clear crypto accelerator statistics
>
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clear crypto protocol statistics</td>
<td>Clears the protocol-specific statistics in the crypto accelerator MIB.</td>
</tr>
<tr>
<td></td>
<td>show crypto accelerator statistics</td>
<td>Displays the global and accelerator-specific statistics in the crypto accelerator MIB.</td>
</tr>
<tr>
<td></td>
<td>show crypto protocol statistics</td>
<td>Displays the protocol-specific statistics from the crypto accelerator MIB.</td>
</tr>
</tbody>
</table>
clear crypto ca crls

To empty the CRL cache of all CRLs associated with a specified trustpoint, all CRLs associated with the trustpool from the cache, or the CRL cache of all CRLs, use the clear crypto ca crls command.

```
clear crypto ca crls [trustpool | trustpoint trust_point_name]
```

**Syntax Description**

| trustpoint | The name of a trustpoint. If you do not specify a name, this command clears all CRLs cached on the system. If you give the trustpoint keyword without a trustpoint name, the command fails. |
| trust_point_name |

| trustpool | Indicates that the action should be applied only to the CRLs that are associated with certificates in the trustpool. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following independent examples clear all of the trustpool CRLs, clears all of the CRLs associated with trustpoint123, and removes all of the cached CRLs from the device:

```
> clear crypto ca crl trustpool
> clear crypto ca crl trustpoint trustpoint123
> clear crypto ca crl
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show crypto ca crl</td>
<td>Displays all cached CRLs or CRLs cached for a specified trustpoint.</td>
</tr>
</tbody>
</table>
clear crypto ca trustpool

To remove all certificates from the trustpool, use the clear crypto ca trustpool command.

clear crypto ca trustpool  noconfirm

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>noconfirm</td>
<td>Suppresses user confirmation prompts, and the command will be processed as requested.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example clears all certificates:

> clear crypto ca trustpool
>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca trustpool export</td>
<td>Exports the certificates that constitute the PKI trustpool.</td>
</tr>
<tr>
<td>crypto ca trustpool import</td>
<td>Imports the certificates that constitute the PKI trustpool.</td>
</tr>
<tr>
<td>crypto ca trustpool remove</td>
<td>Removes a single specified certificate from the trustpool.</td>
</tr>
</tbody>
</table>
clear crypto ikev1

To remove the IPsec IKEv1 SAs or statistics, use the **clear crypto ikev1** command.

```
clear crypto ikev1  { sa  [ ip_address ]  |  stats }
```

**Syntax Description**

- `sa ip_address` Clears the SA. To clear all IKEv1 SAs, use this option without specifying an IP address. Otherwise, specify the IPv4 or IPv6 address of the SA to clear.
- `stats` Clears the IKEv1 statistics.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example removes all of the IPsec IKEv1 statistics from the Firepower Threat Defense device:

```
> clear crypto ikev1 stats
>
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
> clear crypto ikev1 sa 10.86.1.1
>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipsec sa</td>
<td>Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.</td>
</tr>
<tr>
<td>show running-config crypto</td>
<td>Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.</td>
</tr>
</tbody>
</table>
clear crypto ikev2

To remove the IPsec IKEv2 SAs or statistics, use the **clear crypto ikev2** command.

```
clear crypto ikev2 {sa [ip_address] | stats}
```

**Syntax Description**

- `sa ip_address` Clears the SA. To clear all IKEv2 SAs, use this option without specifying an IP address. Otherwise, specify the IPv4 or IPv6 address of the SA to clear.

- `stats` Clears the IKEv2 statistics.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example removes all of the IPsec IKEv2 statistics from the Firepower Threat Defense device:

```
> clear crypto ikev2 stats
>
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
> clear crypto ikev2 sa 10.86.1.1
>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipsec sa</code></td>
<td>Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.</td>
</tr>
<tr>
<td><code>show running-config crypto</code></td>
<td>Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.</td>
</tr>
</tbody>
</table>
clear crypto ipsec sa

To remove the IPsec SA counters, entries, crypto maps or peer connections, use the clear crypto ipsec sa command.

```
clear crypto ipsec sa [counters | entry ip_address {esp | ah} spi | inactive | map map_name | peer ip_address]
```

**Syntax Description**

- `ah` Authentication header.
- `counters` Clears all IPsec per SA statistics.
- `entry ip_address` Deletes the tunnel that matches the specified IP address/hostname, and protocol, and SPI value.
- `esp` Encryption security protocol.
- `inactive` Clears all inactive IPsec SAs.
- `map map_name` Deletes all tunnels associated with the specified crypto map as identified by map name.
- `peer ip_address` Deletes all IPsec SAs to a peer as identified by the specified hostname or IP address.
- `spi` Identifies the Security Parameters Index (a hexadecimal number). This must be the inbound SPI. We do not support this command for the outbound SPI.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To clear all IPsec SAs, use this command without arguments.

**Examples**

The following example removes all of the IPsec SAs from the Firepower Threat Defense:

```
> clear crypto ipsec sa
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
> clear crypto ipsec sa peer 10.86.1.1
```
## clear crypto ipsec sa

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipsec sa</td>
<td>Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.</td>
</tr>
<tr>
<td>show running-config crypto</td>
<td>Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.</td>
</tr>
</tbody>
</table>
clear crypto isakmp

To clear ISAKMP SAs or statistics, use the clear crypto isakmp command.

clear crypto isakmp [sa | stats]

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sa</td>
</tr>
<tr>
<td>stats</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
</tr>
<tr>
<td>Modification</td>
</tr>
<tr>
<td>6.1</td>
</tr>
<tr>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>To clear all ISAKMP operational data, use this command without arguments.</td>
</tr>
</tbody>
</table>

Examples
The following example removes all of the ISAKMP SAs:

> clear crypto isakmp sa
>

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
</tr>
<tr>
<td>show isakmp</td>
</tr>
<tr>
<td>show running-config crypto</td>
</tr>
</tbody>
</table>
clear crypto protocol statistics

To clear the protocol-specific statistics in the crypto accelerator MIB, use the clear crypto protocol statistics command.

clear crypto protocol statistics protocol

**Syntax Description**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All protocols currently supported.</td>
</tr>
<tr>
<td>ikev1</td>
<td>Internet Key Exchange (IKE) version 1.</td>
</tr>
<tr>
<td>ikev2</td>
<td>Internet Key Exchange (IKE) version 2.</td>
</tr>
<tr>
<td>ipsec</td>
<td>IP Security (IPsec) Phase-2 protocols.</td>
</tr>
<tr>
<td>other</td>
<td>Reserved for new protocols.</td>
</tr>
<tr>
<td>srtp</td>
<td>Secure RTP (SRTP) protocol</td>
</tr>
<tr>
<td>ssh</td>
<td>Secure Shell (SSH) protocol</td>
</tr>
<tr>
<td>ssl</td>
<td>Secure Socket Layer (SSL) protocol</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears all crypto accelerator statistics:

```
> clear crypto protocol statistics all
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crypto accelerator statistics</td>
<td>Clears the global and accelerator-specific statistics in the crypto accelerator MIB.</td>
</tr>
<tr>
<td>show crypto accelerator statistics</td>
<td>Displays the global and accelerator-specific statistics from the crypto accelerator MIB.</td>
</tr>
<tr>
<td>show crypto protocol statistics</td>
<td>Displays the protocol-specific statistics in the crypto accelerator MIB.</td>
</tr>
</tbody>
</table>
clear crypto ssl

To clear SSL information, use the `clear crypto ssl` command.

```
clear crypto ssl { cache [all] | errors | mib | objects }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache</td>
<td>Clears expired sessions in the SSL session cache.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Clears all sessions and statistics in the SSL session cache.</td>
</tr>
<tr>
<td>errors</td>
<td>Clears SSL errors.</td>
</tr>
<tr>
<td>mib</td>
<td>Clears SSL MIB statistics.</td>
</tr>
<tr>
<td>objects</td>
<td>Clears SSL object statistics.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example clears all SSL cache sessions and statistics:

```
> clear crypto ssl cache all
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show crypto ssl</td>
<td>Displays the SSL information.</td>
</tr>
</tbody>
</table>
clear dhcpd

To clear the DHCP server bindings and statistics, use the clear dhcpd command.

```
clear dhcpd { binding [all | ip_address] | statistics }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) Clears all dhcpd bindings.</td>
</tr>
<tr>
<td>binding</td>
<td>Clears all the client address bindings.</td>
</tr>
<tr>
<td>ip_address</td>
<td>(Optional) Clears the binding for the specified IP address.</td>
</tr>
<tr>
<td>statistics</td>
<td>Clears statistical information counters.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to clear the dhcpd statistics:

```
> clear dhcpd statistics
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dhcpd</td>
<td>Displays DHCP binding, statistic, or state information.</td>
</tr>
</tbody>
</table>
clear dhcprelay statistics

To clear the DHCP relay statistic counters, use the **clear dhcprelay statistics** command.

**clear dhcprelay statistics**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to clear the DHCP relay statistics:

```
> clear dhcprelay statistics
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dhcprelay statistics</td>
<td>Displays DHCP relay agent statistic information.</td>
</tr>
<tr>
<td>show running-config dhcprelay</td>
<td>Displays the current DHCP relay agent configuration.</td>
</tr>
</tbody>
</table>
clear dns

To clear all IP addresses associated with the specified fully qualified domain name (FQDN) host, use the `clear dns` command.

`clear dns [host  fqdn_name]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host  fqdn_name</td>
<td>(Optional) Specifies the fully qualified domain name whose IP addresses you want to clear. If you do not specify a host, all DNS resolutions are cleared.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears the IP addresses associated with the specified FQDN host:

```
> clear dns host www.example.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dns-hosts</td>
<td>Shows the DNS cache.</td>
</tr>
</tbody>
</table>
clear dns-hosts cache

To clear the DNS cache, use the clear dns-hosts cache command.

```
clear dns-hosts cache
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example clears the DNS cache:

```
> clear dns-hosts cache
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dns-hosts</td>
<td>Shows the DNS cache.</td>
</tr>
</tbody>
</table>
clear eigrp events

To clear the EIGRP event log, use the `clear eigrp events` command.

```plaintext
clear eigrp [as_number] events
```

**Syntax Description**

| as_number | (Optional) Specifies the autonomous system number of the EIGRP process for which you are clearing the event log. Because the device only supports one EIGRP routing process, you do not need to specify the autonomous system number (process ID). |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use the `show eigrp events` command to view the EIGRP event log.

**Examples**

The following example clears the EIGRP event log:

```plaintext
> clear eigrp events
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show eigrp events</td>
<td>Displays the EIGRP event log.</td>
</tr>
</tbody>
</table>
clear eigrp neighbors

To delete entries from the EIGRP neighbor table, use the `clear eigrp neighbors` command.

```
clear eigrp [as_number] neighbors [ip_addr | if_name] [soft]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>as_number</code></td>
<td>(Optional) Specifies the autonomous system number of the EIGRP process for which you are deleting neighbor entries. Because the device only supports one EIGRP routing process, you do not need to specify the autonomous system number (AS), which is the process ID.</td>
</tr>
<tr>
<td><code>if_name</code></td>
<td>(Optional) The name of an interface. Specifying an interface name removes all neighbor table entries that were learned through this interface.</td>
</tr>
<tr>
<td><code>ip_addr</code></td>
<td>(Optional) The IP address of the neighbor you want to remove from the neighbor table.</td>
</tr>
<tr>
<td><code>soft</code></td>
<td>Causes the device to resynchronize with the neighbor without resetting the adjacency.</td>
</tr>
</tbody>
</table>

**Command Default**

If you do not specify a neighbor IP address or an interface name, all dynamic entries are removed from the neighbor table.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `clear eigrp neighbors` command does not remove neighbors that were manually defined from the neighbor table. Only dynamically discovered neighbors are removed.

You can use the `show eigrp neighbors` command to view the EIGRP neighbor table.

**Examples**

The following example removes all entries from the EIGRP neighbor table:

```
> clear eigrp neighbors
```

The following example removes all entries learned through the interface named “outside” from the EIGRP neighbor table:

```
> clear eigrp neighbors outside
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show eigrp neighbors</code></td>
<td>Displays the EIGRP neighbor table.</td>
</tr>
</tbody>
</table>
clear eigrp topology

To delete entries from the EIGRP topology table, use the `clear eigrp topology` command.

```plaintext
clear eigrp [as_number] topology ip_addr [mask]
```

**Syntax Description**
- `as_number` (Optional) Specifies the autonomous system number of the EIGRP process. Because the device only supports one EIGRP routing process, you do not need to specify the autonomous system number (AS), which is the process ID.
- `ip_addr` The IP address to clear from the topology table.
- `mask` (Optional) The network mask to apply to the `ip-addr` argument.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command clears existing EIGRP entries from the EIGRP topology table. You can use the `show eigrp topology` command to view the topology table entries.

**Examples**

The following example removes entries in the 192.168.1.0 network from EIGRP topology table:

```plaintext
> clear eigrp topology 192.168.1.0 255.255.255.0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show eigrp topology</code></td>
<td>Displays the EIGRP topology table.</td>
</tr>
</tbody>
</table>
clear f - clear z

- clear facility-alarm output, on page 75
- clear failover statistics, on page 76
- clear flow-export counters, on page 77
- clear flow-offload, on page 78
- clear fragment, on page 79
- clear gc, on page 80
- clear igmp, on page 81
- clear ikev1, on page 82
- clear ikev2, on page 83
- clear interface, on page 84
- clear ip, on page 85
- clear ipsec sa, on page 86
- clear ipv6 dhcp, on page 88
- clear ipv6 dhcprelay, on page 89
- clear ipv6 mld traffic, on page 90
- clear ipv6 neighbors, on page 91
- clear ipv6 ospf, on page 92
- clear ipv6 prefix-list, on page 93
- clear ipv6 route, on page 94
- clear ipv6 traffic, on page 95
- clear isakmp, on page 96
- clear isis, on page 97
- clear kernel cgroup-controller, on page 99
- clear lacp, on page 100
- clear lisp eid, on page 101
- clear local-host, on page 102
- clear logging, on page 103
- clear mac-address-table, on page 104
- clear memory, on page 105
- clear mfib counters, on page 106
- clear nat counters, on page 107
- clear object-group, on page 108
- clear ospf, on page 109
• clear packet debugs, on page 110
• clear packet-tracer, on page 111
• clear pclu, on page 112
• clear pim, on page 113
• clear prefix-list, on page 115
• clear priority-queue statistics, on page 116
• clear process, on page 117
• clear resource usage, on page 118
• clear route, on page 120
• clear rule hits, on page 121
• clear service-policy, on page 122
• clear service-policy inspect gtp, on page 123
• clear service-policy inspect m3ua, on page 125
• clear service-policy inspect radius-accounting, on page 126
• clear shun, on page 127
• clear snmp-server statistics, on page 128
• clear snort statistics, on page 129
• clear snort tls-offload, on page 130
• clear ssl, on page 131
• clear sunrpc-server active, on page 132
• clear threat-detection rate, on page 133
• clear threat-detection scanning-threat, on page 134
• clear threat-detection shun, on page 135
• clear threat-detection statistics, on page 136
• clear traffic, on page 137
• clear vpn-sessiondb statistics, on page 138
• clear wccp, on page 140
• clear webvpn statistics, on page 141
• clear xlate, on page 142
clear facility-alarm output

To de-energize the output relay and clear the alarm state of the LED in the ISA 3000, use the **clear facility-alarm output** command

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command de-energizes the output relay and clears the alarm state of the output LED. This turns off the external alarm. However, this command does not fix the alarm condition that triggered the external alarm: you still must resolve the problem. Use the **show facility-alarm status** command to determine the current alarm conditions.

### Examples

The following example de-energizes the output relay and clears the alarm state of the output LED:

```plaintext
> clear facility-alarm output
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show alarm settings</strong></td>
<td>Displays all global alarm settings.</td>
</tr>
<tr>
<td><strong>show environment alarm-contact</strong></td>
<td>Displays the status of the input alarm contacts.</td>
</tr>
<tr>
<td><strong>show facility-alarm</strong></td>
<td>Displays status information for triggered alarms.</td>
</tr>
</tbody>
</table>
clear failover statistics

To clear the high availability statistic counters, use the **clear failover statistics** command.

**clear failover statistics**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command clears the statistics displayed with the **show failover statistics** command and the counters in the Stateful Failover Logical Update Statistics section of the **show failover** command output.

**Examples**

The following example shows how to clear the high availability statistic counters:

```plaintext
> clear failover statistics
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show failover</td>
<td>Displays information about the high availability configuration and operational statistics.</td>
</tr>
</tbody>
</table>
clear flow-export counters

To reset runtime counters for NetFlow statistical and error data to zero, use the `clear flow-export counters` command.

```
clear flow-export counters
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to reset NetFlow runtime counters:

```
> clear flow-export counters
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show flow-export counters</td>
<td>Displays all NetFlow runtime counters.</td>
</tr>
</tbody>
</table>
clear flow-offload

To clear counters and statistics for offloaded flows, use the `clear flow-offload` command. This command is available on Firepower Threat Defense on the Firepower 4100/9300 chassis.

`clear flow-offload statistics`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>statistics</th>
<th>Resets to zero statistics for all offloaded flows.</th>
</tr>
</thead>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

Following is an example of clearing all flow counters:

```plaintext
> clear flow-offload statistics
```

**Related Commands**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show flow-offload</code></td>
<td>Displays dynamic flow offload counters, statistics, and information.</td>
</tr>
<tr>
<td><code>configure flow-offload</code></td>
<td>Enables or disables dynamic flow offload.</td>
</tr>
</tbody>
</table>
clear fragment

To clear the operational data of the IP fragment reassembly module, enter the `clear fragment` command.

```
clear fragment  { queue  |  statistics  [ interface_name ] }
```

**Syntax Description**

- `queue` Clears the IP fragment reassembly queue.
- `statistics interface_name` Clears the IP fragment reassembly statistics. You can optionally specify an interface name to clear statistics for that interface only. Otherwise, statistics for all interfaces are cleared.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command clears either the currently queued fragments that are waiting for reassembly (if the `queue` keyword is entered) or clears all IP fragment reassembly statistics (if the `statistics` keyword is entered). The statistics are the counters, which tell how many fragments chains were successfully reassembled, how many chains failed to be reassembled, and how many times the maximum size was crossed resulting in overflow of the buffer.

**Examples**

The following example shows how to clear the operational data of the IP fragment reassembly module:

```
> clear fragment queue
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show fragment</code></td>
<td>Displays the operational data of the IP fragment reassembly module.</td>
</tr>
<tr>
<td><code>show running-config fragment</code></td>
<td>Displays the IP fragment reassembly configuration.</td>
</tr>
</tbody>
</table>
clear gc

To remove the garbage collection (GC) process statistics, use the `clear gc` command.

clear gc

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to remove the GC process statistics:

> clear gc

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show gc</td>
<td>Displays the GC process statistics.</td>
</tr>
</tbody>
</table>
### clear igmp

To clear all IGMP counters, group caches, and traffic, use the **clear igmp** command.

```
clear igmp {counters [if_name] | group [interface name] | traffic}
```

#### Syntax Description

- **counters [if_name]**: Clears IGMP statistical counters. You can optionally specify an interface name to clear the counters for that interface only.

- **group [interface name]**: Deletes IGMP group cache entries. You can optionally specify an interface name to delete the groups associated with that interface only.

  This command does not clear statically configured groups.

- **traffic**: Clears traffic counters.

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Examples

The following example clears the IGMP statistical counters:

```
> clear igmp counters
```

The following example shows how to clear all discovered IGMP groups from the IGMP group cache:

```
> clear igmp group
```

The following example clears the IGMP statistical traffic counters:

```
> clear igmp traffic
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp</td>
<td>Shows IGMP information.</td>
</tr>
</tbody>
</table>
clear ikev1

To remove the IPsec IKEv1 SAs or statistics, use the `clear ikev1` command.

```
clear ikev1 { sa [ip_address] | stats }
```

**Syntax Description**

- `sa ip_address` Clears the SA. To clear all IKEv1 SAs, use this option without specifying an IP address. Otherwise, specify the IPv4 or IPv6 address of the SA to clear.

- `stats` Clears the IKEv1 statistics.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example removes all of the IPsec IKEv1 statistics from the Firepower Threat Defense device:

```
> clear ikev1 stats
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
> clear ikev1 sa 10.86.1.1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipsec sa</code></td>
<td>Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.</td>
</tr>
<tr>
<td><code>show running-config crypto</code></td>
<td>Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.</td>
</tr>
</tbody>
</table>
clear ikev2

To remove the IPsec IKEv2 SAs or statistics, use the clear ikev2 command.

```
clear ikev2 { sa [ip_address] | stats }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sa ip_address</code></td>
<td>Clears the SA. To clear all IKEv2 SAs, use this option without specifying an IP address. Otherwise, specify the IPv4 or IPv6 address of the SA to clear.</td>
</tr>
<tr>
<td><code>stats</code></td>
<td>Clears the IKEv2 statistics.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example removes all of the IPsec IKEv2 statistics from the Firepower Threat Defense device:

```
> clear ikev2 stats
>
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
> clear ikev2 sa 10.86.1.1
>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipsec sa</code></td>
<td>Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.</td>
</tr>
<tr>
<td><code>show running-config crypto</code></td>
<td>Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.</td>
</tr>
</tbody>
</table>
clear interface

To clear interface statistics, use the `clear interface` command.

```
clear interface  [physical_interface [ .subinterface ]  |  interface_name ]
```

**Syntax Description**

- `interface_name` (Optional) Identifies the interface name.
- `physical_interface` (Optional) Identifies the interface ID, such as `gigabitethernet0/1`.
- `subinterface` (Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

**Command Default**

By default, this command clears all interface statistics.

**Command History**

- **Release**  
  **Modification**
  
  | 6.1  | This command was introduced. |

**Examples**

The following example clears all interface statistics:

```
> clear interface
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interface</code></td>
<td>Displays the runtime status and statistics of interfaces.</td>
</tr>
<tr>
<td><code>show running-config interface</code></td>
<td>Displays the interface configuration.</td>
</tr>
</tbody>
</table>
clear ip

To clear statistics for certain legacy features, use the clear ip command.

```
clear ip (audit count [global] | verify statistics) [interface interface_name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>clear ip</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit count [global]</td>
<td>Clears the count of signature matches for an audit policy. If you do not specify the interface keyword, counts for all signatures are cleared globally. You can optionally include the global keyword to specify this explicitly (you cannot specify both global and interface).</td>
</tr>
<tr>
<td>interface interface_name</td>
<td>(Optional) Clear statistics for the specified interface only.</td>
</tr>
<tr>
<td>verify statistics</td>
<td>Clears the number of packets dropped for Unicast Reverse Path Forwarding (RPF).</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

These features are normally not enabled, so typically there are no statistics to clear.

**Example**

The following example clears the IP audit count for all interfaces.

```
> clear ip audit count
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip audit count</td>
<td>Displays the Unicast RPF statistics.</td>
</tr>
<tr>
<td>show ip verify statistics</td>
<td>Displays the Unicast RPF statistics.</td>
</tr>
<tr>
<td>show running-config ip audit name</td>
<td>Shows the configuration for the ip audit name command. Besides name, you can check on the interface and signature configuration.</td>
</tr>
<tr>
<td>show running-config ip verify reverse-path</td>
<td>Shows the ip verify reverse-path configuration.</td>
</tr>
</tbody>
</table>
clear ipsec sa

To remove the IPsec SA counters, entries, crypto maps or peer connections, use the **clear ipsec sa** command.

```plaintext
clear ipsec sa [counters | entry ip_address {esp | ah} spi | inactive | map map_name | peer ip_address]
```

### Syntax Description

- **ah**
  - Authentication header.
- **counters**
  - Clears all IPsec per SA statistics.
- **entry ip_address**
  - Deletes the tunnel that matches the specified IP address/hostname, and protocol, and SPI value.
- **esp**
  - Encryption security protocol.
- **inactive**
  - Clears all inactive IPsec SAs.
- **map map_name**
  - Deletes all tunnels associated with the specified crypto map as identified by map name.
- **peer ip_address**
  - Deletes all IPsec SAs to a peer as identified by the specified hostname or IP address.
- **spi**
  - Identifies the Security Parameters Index (a hexadecimal number). This must be the inbound SPI. We do not support this command for the outbound SPI.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To clear all IPsec SAs, use this command without arguments.

### Examples

The following example, issued in global configuration mode, removes all of the IPsec SAs from the Firepower Threat Defense:

```plaintext
> clear ipsec sa
>
```

The following example, entered in global configuration mode, deletes SAs with a peer IP address of 10.86.1.1:

```plaintext
> clear ipsec sa peer 10.86.1.1
```
## A - R Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipsec sa</code></td>
<td>Displays information about IPsec SAs, including counters, entry, map name, peer IP address and hostname.</td>
</tr>
<tr>
<td><code>show running-config crypto</code></td>
<td>Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.</td>
</tr>
</tbody>
</table>
clear ipv6 dhcp

To clear DHCPv6 statistics, use the clear ipv6 dhcp command.

```
clear ipv6 dhcp { client [ pd ] | interface interface_name | server } statistics
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client [ pd ]</td>
<td>Clears the DHCPv6 client statistics. Add the pd keyword to clear the Prefix Delegation client statistics.</td>
</tr>
<tr>
<td>interface</td>
<td>interface_name</td>
</tr>
<tr>
<td>server</td>
<td>Clears the DHCPv6 server statistics.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

The following example clears the DHCPv6 client statistics:

```
> clear ipv6 dhcp client statistics
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 dhcp</td>
<td>Shows DHCPv6 statistics.</td>
</tr>
</tbody>
</table>
clear ipv6 dhcprelay

To clear the IPv6 DHCP relay binding entries and statistics, use the `clear ipv6 dhcprelay` command.

```
clear ipv6 dhcprelay {binding [ip_address] | statistics}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>binding</td>
<td>Clears the IPv6 DHCP relay binding entries.</td>
</tr>
<tr>
<td>ip_address</td>
<td>(Optional) Specifies the IPv6 address for the DHCP relay binding. If the IP address is specified, only the relay binding entries associated with that IP address are cleared.</td>
</tr>
<tr>
<td>statistics</td>
<td>Clears the IPv6 DHCP relay agent statistics.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to clear the statistical data for the IPv6 DHCP relay binding:

```
> clear ipv6 dhcprelay binding
>
```

The following example shows how to clear the statistical data for the IPv6 DHCP relay agent:

```
> clear ipv6 dhcprelay statistics
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 dhcprelay</td>
<td>Shows the relay binding entries created by the relay agent.</td>
</tr>
<tr>
<td>show ipv6 dhcprelay</td>
<td>Shows the IPv6 DHCP relay agent information.</td>
</tr>
<tr>
<td>binding</td>
<td></td>
</tr>
<tr>
<td>statistics</td>
<td></td>
</tr>
</tbody>
</table>
clear ipv6 mld traffic

To clear the IPv6 Multicast Listener Discovery (MLD) traffic counters and reset them, use the clear ipv6 mld traffic command.

**clear ipv6 mld traffic**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the traffic counters for IPv6 MLD:

> clear ipv6 mld traffic
>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 mld traffic</td>
<td>Show IPv6 MLD traffic counters.</td>
</tr>
</tbody>
</table>
clear ipv6 neighbors

To clear the IPv6 neighbor discovery cache, use the **clear ipv6 neighbors** command.

clear ipv6 neighbors

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command deletes all discovered IPv6 neighbor from the cache; it does not remove static entries.

**Examples**

The following example deletes all entries, except static entries, in the IPv6 neighbor discovery cache:

```
> clear ipv6 neighbors
>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 neighbor</td>
<td>Displays IPv6 neighbor cache information.</td>
</tr>
</tbody>
</table>
clear ipv6 ospf

To clear OSPFv3 routing parameters, use the clear ipv6 ospf command.

```
clear ipv6 [process_id] [counters] [events] [force-spf] [process] [redistribution] [traffic]
```

**Syntax Description**
- **counters**: Resets the OSPF process counters.
- **events**: Clears the OSPF event log.
- **force-ospf**: Clears the SPF for OSPF processes.
- **process**: Resets the OSPFv3 process.
- **process_id**: Clears the process ID number. Valid values range from 1 to 65535.
- **redistribution**: Clears OSPFv3 route redistribution.
- **traffic**: Clears traffic-related statistics.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to clear all OSPFv3 route redistribution:

```
> clear ipv6 ospf redistribution
>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Shows the running configuration of OSPFv3 processes.</td>
</tr>
<tr>
<td>ipv6 router</td>
<td></td>
</tr>
</tbody>
</table>
clear ipv6 prefix-list

To clear routing IPv6 prefix-lists, use the **clear ipv6 prefix-list** command.

**clear ipv6 prefix-list**   [name]

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Clears the named IPv6 prefix-list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to clear the list1 IPv6 prefix-list:

```
> clear ipv6 prefix-list list1
>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Shows the running configuration of IPv6 prefix-lists.</td>
</tr>
<tr>
<td>ipv6 prefix-list</td>
<td></td>
</tr>
</tbody>
</table>
clear ipv6 route

To delete routes from the IPv6 routing table, use the clear ipv6 route command.

```
clear ipv6 route [management-only] {all | ipv6-prefix/prefix-length}
```

**Syntax Description**
- **management-only**: Clears only the IPv6 management routing table.
- **ipv6-prefix/prefix-length**: Clears routed for the IPv6 prefix.
- **all**: Clears all IPv6 routes.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `clear ipv6 route` command is similar to the `clear ip route` command, except that it is IPv6-specific. The per-destination maximum transmission unit (MTU) cache is also cleared.

**Examples**
The following example deletes the IPv6 route for 2001:0DB8::/35:

```
> clear ipv6 route 2001:0DB8::/35
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 route</td>
<td>Displays IPv6 routes.</td>
</tr>
</tbody>
</table>
clear ipv6 traffic

To reset the IPv6 traffic counters, use the `clear ipv6 traffic` command.

```
clear ipv6 traffic
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Using this command resets the counters in the output from the `show ipv6 traffic` command.

**Examples**

The following example resets the IPv6 traffic counters.

```
> clear ipv6 traffic
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 traffic</td>
<td>Displays IPv6 traffic statistics.</td>
</tr>
</tbody>
</table>
clear isakmp

To clear ISAKMP SAs or statistics, use the `clear isakmp` command.

```
clear isakmp [sa | stats]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sa</td>
<td>(Optional) Clears IKEv1 and IKEv2 SAs.</td>
</tr>
<tr>
<td>stats</td>
<td>(Optional) Clears IKEv1 and IKEv2 statistics.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To clear all ISAKMP operational data, use this command without arguments.

**Examples**

The following example removes all of the ISAKMP SAs:

```
> clear isakmp sa
> clear isakmp sa
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show isakmp</td>
<td>Displays information about ISAKMP operational data.</td>
</tr>
<tr>
<td>show running-config crypto</td>
<td>Displays the entire crypto configuration, including IPsec, crypto maps,</td>
</tr>
<tr>
<td></td>
<td>dynamic crypto maps, and ISAKMP.</td>
</tr>
</tbody>
</table>
clear isis

To clear the IS-IS data structures, use the **clear isis** command.

```
clear isis [ * | lspfull | rib redistribution [level-1 | level-2] [network_prefix] [network_mask] ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Clears all IS-IS data structures.</td>
</tr>
<tr>
<td>level-1</td>
<td>(Optional) Clears Level 1 IS-IS redistributed prefixes from the redistribution cache.</td>
</tr>
<tr>
<td>level-2</td>
<td>(Optional) Clears Level 2 IS-IS redistributed prefixes from the redistribution cache.</td>
</tr>
<tr>
<td>lspfull</td>
<td>Clears the IS-IS LSPFULL state.</td>
</tr>
<tr>
<td>network_mask</td>
<td>(Optional) The network ID in the A.B.C.D format for the network mask for the specific network prefix you want to clear from the RIB. If you do not provide a network mask for the prefix, the major net of the prefix will be used for the network mask.</td>
</tr>
<tr>
<td>network_prefix</td>
<td>(Optional) The network ID in the A.B.C.D format for the specific network prefix you want to clear from the redistribution Routing Information Base (RIB). If you do not provide a network mask for the prefix, the major net of the prefix will be used for the network mask.</td>
</tr>
<tr>
<td>rib redistribution</td>
<td>Clears prefixes in the IS-IS redistribution cache.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the link-state PDU (LSP) becomes full because too many routes are redistributed, use the **clear isis lspfull** command to clear the state after the problem has been resolved.

We recommend that you use the **clear isis rib** command in a troubleshooting situation only when a Cisco Technical Assistance Center representative requests you to do so following a software error.

**Examples**

The following example clears the LSPFULL state:

```
> clear isis lspfull
```

The following example clears the network prefix 10.1.0.0 from the IP local redistribution cache:

```
> clear isis rib redistribution 10.1.0.0 255.255.0.0
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show clns</code></td>
<td>Shows CLNS-specific information.</td>
</tr>
<tr>
<td><code>show isis</code></td>
<td>Shows IS-IS information.</td>
</tr>
<tr>
<td><code>show route isis</code></td>
<td>Shows IS-IS routes.</td>
</tr>
</tbody>
</table>

**Note:**
- `clear isis` is not listed as a related command in the provided text.
clear kernel cgroup-controller

To clear the kernel’s cgroup controller statistics, use the clear kernel cgroup-controller command.

clear kernel cgroup-controller  [cpu | memory]

Syntax Description

<table>
<thead>
<tr>
<th>CPU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu</td>
<td>(Optional) Clears the cpu/cpuacct controller statistics.</td>
</tr>
<tr>
<td>memory</td>
<td>(Optional) Clears memory controller statistics.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to clear the cgroup-controller statistics:

> clear kernel cgroup-controller

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show kernel cgroup-controller</td>
<td>Displays cgroup controller statistics.</td>
</tr>
</tbody>
</table>
clear lacp

To clear EtherChannel LACP port channel statistics, use the clear lacp command.

clear lacp [channel_group_number]

Syntax Description

channel_group_number (Optional.) Clears the channel group information by number, between 1 and 48.

Command Default

If you do not specify a number, statistics for all port channels are cleared.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to clear the port channel statistics:

> clear lacp 12

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lacp</td>
<td>Displays port channel information.</td>
</tr>
</tbody>
</table>
clear lisp eid

To clear the Lisp EID table, use the clear list eid command.

clear lisp eid [ip_address]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
</tr>
<tr>
<td>Removes the specified IP address from the EID table.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
</tr>
<tr>
<td>Modification</td>
</tr>
<tr>
<td>6.2</td>
</tr>
<tr>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The device maintains an EID table that correlates the EID and the site ID. The clear lisp eid command clears EID entries in the table.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear cluster info</td>
<td>Clears the flow mobility counters.</td>
</tr>
<tr>
<td>flow-mobility counters</td>
<td></td>
</tr>
<tr>
<td>show cluster info</td>
<td>Shows flow mobility counters.</td>
</tr>
<tr>
<td>flow-mobility counters</td>
<td></td>
</tr>
<tr>
<td>show conn</td>
<td>Shows traffic subject to LISP flow-mobility.</td>
</tr>
<tr>
<td>show lisp eid</td>
<td>Shows the EID table.</td>
</tr>
</tbody>
</table>
# clear local-host

To reinitialize per-client run-time states such as connection limits and embryonic limits, use the `clear local-host` command.

```
clear local-host [hostname | ip_address] [all] [zone]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) Clears all connections, including to-the-box traffic. Without the <code>all</code> keyword, only through-the-box traffic is cleared.</td>
</tr>
<tr>
<td>hostname or ip_address</td>
<td>(Optional) Specifies the local hostname or IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>zone</td>
<td>(Optional) Clears all connections in traffic zones.</td>
</tr>
</tbody>
</table>

**Command Default**

Clears all through-the-box run-time states.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you make security policy changes to the configuration, all new connections use the new security policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy using the `clear local-host` command. You can alternatively use the `clear conn` command for more granular connection clearing, or the `clear xlate` command for connections that used dynamic NAT.

The `clear local-host` command releases the hosts from the host license limit. You can see the number of hosts that are counted toward the license limit by entering the `show local-host` command.

**Examples**

The following example clears the run-time state and associated connections for the host 10.1.1.15:

```
> clear local-host 10.1.1.15
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear conn</td>
<td>Terminates connections in any state.</td>
</tr>
<tr>
<td>clear xlate</td>
<td>Clears a dynamic NAT session, and any connections using NAT.</td>
</tr>
<tr>
<td>show local-host</td>
<td>Displays the network states of local hosts.</td>
</tr>
</tbody>
</table>
clear logging

To clear the logging buffer, use the clear logging command.

clear logging \{buffer | queue bufferwrap | unified-client\}

Syntax Description

- **buffer**: Clears the internal logging buffer.
- **queue bufferwrap**: Clears the saved FTP and flash logging buffer queues.
- **unified-client**: Clears the logging statistics from the unified logging client, loggerD.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.3</td>
<td>The <strong>unified-client</strong> keyword was added.</td>
</tr>
</tbody>
</table>

Examples

This example shows how to clear the contents of the log buffer:

```
> clear logging buffer
```

The following example shows how to clear the contents of the saved log buffers:

```
> clear logging queue bufferwrap
```

The following example shows how to clear the statistics of loggerD service:

```
> clear logging unified-client
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging savelog</td>
<td>Specify an optional flash file name.</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays logging information.</td>
</tr>
</tbody>
</table>
clear mac-address-table

To clear dynamic MAC address table entries, use the clear mac-address-table command.

```
clear mac-address-table [interface_name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface_name</td>
<td>(Optional) Clears the MAC address table entries for the selected interface.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears the dynamic MAC address table entries:

```
> clear mac-address-table
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac-address-table</td>
<td>Shows MAC address table entries.</td>
</tr>
</tbody>
</table>
clear memory

To clear the queues and statistics for a memory tool, use the clear memory command.

```
clear memory  {delayed-free-poisoner | profile [peak] | tracking}
```

**Syntax Description**
- **delayed-free-poisoner**: Returns all memory held in the delayed free-memory poisoner tool queue to the system without validation and clears the related statistical counters. You enable this feature using the `memory delayed-free-poisoner enable` command.

- **profile [peak]**: Clears the memory buffers held by the memory profiling function. Include the optional `peak` keyword to clear the contents of the peak memory buffer. Use the `no memory profile enable` command to stop memory profiling before clearing the profile buffers.

- **tracking**: Clears memory tracking information collected by the `memory tracking enable` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
The following example clears the delayed free-memory poisoner tool queue and statistics:

```
> clear memory delayed-free-poisoner
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory</td>
<td>Enables the various memory tools.</td>
</tr>
<tr>
<td>show memory delayed-free-poisoner</td>
<td>Displays a summary of the delayed free-memory poisoner tool queue usage.</td>
</tr>
<tr>
<td>show memory profile</td>
<td>Displays memory profiling results.</td>
</tr>
<tr>
<td>show memory tracking</td>
<td>Displays memory tracking results.</td>
</tr>
</tbody>
</table>
clear mfib counters

To clear Multicast Forwarding Information Base (MFIB) router packet counters, use the **clear mfib counters** command.

```
clear mfib { cluster-stats | counters [source_or_group [source]] }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-stats</td>
<td>Clears MFIB cluster synchronization statistics.</td>
</tr>
<tr>
<td>count</td>
<td>Clears MFIB route and packet count data. When you use <code>count</code> with no arguments, route counters for all routes are cleared.</td>
</tr>
<tr>
<td>source_or_group</td>
<td>(Optional) The source or group IPv4, IPv6, or name. If you specify both, specify the source first. The source address is a unicast address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears all MFIB router packet counters:

```
> clear mfib counters
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib</td>
<td>Displays MFIB route and packet count data.</td>
</tr>
</tbody>
</table>
**clear nat counters**

To clear NAT policy counters, use the `clear nat counters` command.

```plaintext
clear nat counters [interface name] [ip_addr mask | object | object-group name] [translated [interface name] [ip_addr mask | object | object-group name]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface name</td>
<td>(Optional) Specifies the source or destination (translated) interface.</td>
</tr>
<tr>
<td>ip_addr mask</td>
<td>(Optional) Specifies an IP address and subnet mask.</td>
</tr>
<tr>
<td>object name</td>
<td>(Optional) Specifies a network object or service object.</td>
</tr>
<tr>
<td>object-group name</td>
<td>(Optional) Specifies a network object group</td>
</tr>
<tr>
<td>translated</td>
<td>(Optional) Specifies the translated parameters.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to clear the NAT policy counters:

```plaintext
> clear nat counters
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show nat</td>
<td>Displays the protocol stack counters.</td>
</tr>
</tbody>
</table>
clear object-group

To clear the hit counts of objects in a network object group, use the `show object-group` command.

```
clear object-group [object-group name]
```

**Syntax Description**

- `object-group name`:
  - The name of the object group whose counters should be cleared. If you do not specify a group, counters for all object groups are cleared.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the network object hit count for the network object group named “Anet”:

```
> clear object-group Anet
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show object-group</code></td>
<td>Shows object group information and shows hit counts if the specified object group is of the network object-group type.</td>
</tr>
</tbody>
</table>
clear ospf

To clear OSPF process information, use the clear ospf command.

```
clear ospf { counters [ neighbor interface ] | events | force-spf | process / noconfirm | redistribution | traffic }
```

**Syntax Description**
- **counters**: Clears the OSPF counters.
- **neighbor interface**: (Optional) Clears statistics for that neighbor only.
- **events**: Clears the OSPF event log.
- **force-spf**: Clears the incremental SPF statistics.
- **process / noconfirm**: Restart the OSPF routing process.
- **redistribution**: Clears OSPF route redistribution statistics.
- **traffic**: Clears OSPF traffic-related statistics.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command does not remove any part of the configuration, it clears statistics only.

**Examples**

The following example shows how to clear all OSPF neighbor counters:

```console
> clear ospf counters
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ospf</td>
<td>Shows all OSPF information from the running configuration.</td>
</tr>
</tbody>
</table>
clear packet debugs

To remove the debug logs from the database, use the `clear packet debugs` command.

```
clear packet debugs
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `clear packet debugs` command to remove all the debug logs from the database.

**Examples**

The following example shows how to remove all debug logs stored in the debug logs database.

```
> clear packet debugs
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug packet start</td>
<td>Starts writing debug logs to the database.</td>
</tr>
</tbody>
</table>
clear packet-tracer

To remove persistent packet tracers, use the clear packet-tracer command.

clear packet-tracer

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Persistent packet tracers are those you configure with the persist keyword on the packet-tracer command.

Examples

The following example shows how to remove all persistent packet tracers.

> clear packet-tracer
>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packet-tracer</td>
<td>Configures packet tracers.</td>
</tr>
</tbody>
</table>
clear pclu

To clear PC logical update statistics, use the **clear pclu** command.

```markdown
clear pclu
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example clears PC information:

```markdown
> clear pclu
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pclu</td>
<td>Shows PCLU information.</td>
</tr>
</tbody>
</table>
clear pim

To clear PIM traffic counters and mappings, use the `clear pim` command.

```
clear pim { counters | group-map [rp-address] | reset | topology [group] }
```

**Syntax Description**

- **counters**
  
  Clears the PIM traffic counters.

- **group-map [rp-address]**
  
  Deletes group-to-rendezvous point (RP) mapping entries from the RP mapping cache. You can optionally specify the name of a rendezvous point to clear entries for that RP only. The name can be:
  
  - Name of the RP, as defined in the Domain Name System (DNS) hosts table.
  - IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.

- **reset**
  
  Forces MRIB synchronization through reset. All information from the topology table is cleared, and the MRIB connection is reset. You can use this option to synchronize states between the PIM topology table and the MRIB database.

- **topology [group]**
  
  Clears existing PIM routes from the PIM topology table. Information obtained from the MRIB table, such as IGMP local membership, is retained. You can optionally specify the multicast group address or name to be deleted from the topology table. The name can be one of the following:
  
  - Name of the multicast group, as defined in the DNS hosts table.
  - IPv4 or IPv6 address of the multicast group.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears the PIM traffic counters:

```
> clear pim counters
```

The following example deletes group-RP mapping entries at the 23.23.23.2 RP address:

```
> show pim group-map
```

<table>
<thead>
<tr>
<th>Group Range</th>
<th>Proto</th>
<th>Client</th>
<th>Groups</th>
<th>RP address</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.1.39/32*</td>
<td>DM</td>
<td>static</td>
<td>0</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>224.0.1.40/32*</td>
<td>DM</td>
<td>static</td>
<td>0</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/24*</td>
<td>L-Local</td>
<td>static</td>
<td>1</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>222.0.0.0/8*</td>
<td>SSM</td>
<td>config</td>
<td>0</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/4*</td>
<td>SM</td>
<td>config</td>
<td>0</td>
<td>9.9.9.9</td>
<td>RPF: 0.0.0.0</td>
</tr>
</tbody>
</table>
```
224.0.0.0/4   SM   BSR   0   23.23.23.2   RPF: Gi0/3,23.23.23.2
> clear pim group-map 23.23.23.2
> show pim group-map
<table>
<thead>
<tr>
<th>Group Range</th>
<th>Proto</th>
<th>Client</th>
<th>Groups</th>
<th>RP address</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.1.39/32*</td>
<td>DM</td>
<td>static</td>
<td>0</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>224.0.1.40/32*</td>
<td>DM</td>
<td>static</td>
<td>0</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/24*</td>
<td>L-Local</td>
<td>static</td>
<td>1</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>232.0.0.0/8*</td>
<td>SSM</td>
<td>config</td>
<td>0</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/4*</td>
<td>SM</td>
<td>config</td>
<td>0</td>
<td>9.9.9.9</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>SM</td>
<td>static</td>
<td>0</td>
<td>0.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim</td>
<td>Displays PIM traffic information.</td>
</tr>
</tbody>
</table>
clear prefix-list

To reset the hit count of the prefix-list entries, use the `clear prefix-list` command.

```
clear prefix-list [prefix_list_name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>prefix_list_name</th>
<th>(Optional) The name of the prefix list from which the hit count is to be cleared.</th>
</tr>
</thead>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear prefix-list information from a list named `first_list`:

```
> clear prefix-list first_list
>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show prefix-list</td>
<td>Displays information about a prefix list or prefix list entries.</td>
</tr>
</tbody>
</table>
clear priority-queue statistics

To clear the priority-queue statistics counters for an interface or for all configured interfaces, use the clear priority-queue statistics command

```
clear priority-queue statistics  interface_name
```

**Syntax Description**

| interface_name | (Optional) Clears priority-queue statistics for the specified interface. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears priority-queue statistics for all interfaces.

```
> clear priority-queue statistics
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show priority-queue statistics</td>
<td>Shows the priority queue statistics for a specified interface or for all interfaces.</td>
</tr>
</tbody>
</table>
clear process

To clear statistics for specified processes running on the Firepower Threat Defense device, use the clear process command.

```
clear process {cpu-hog | internals}
```

**Syntax Description**
- **cpu-hog**: Clears CPU hogging statistics.
- **internals**: Clears process internal statistics.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to clear CPU hogging statistics:

```
> clear process cpu-hog
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu hog</td>
<td>Triggers real-time CPU hog detection information.</td>
</tr>
<tr>
<td>granular-detection</td>
<td>Triggers real-time CPU hog detection information.</td>
</tr>
<tr>
<td>show processes</td>
<td>Displays a list of the processes that are running on the Firepower Threat Defense.</td>
</tr>
</tbody>
</table>
clear resource usage

To clear resource usage statistics, use the `clear resource usage` command.

```
clear resource usage [ detail | resource { [ rate ] resource_name | all } ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Clears all resource usage details.</td>
</tr>
<tr>
<td>resource [rate]</td>
<td>Clears the usage of a specific resource. Specify <code>all</code> (the default) for all resources. Specify <code>rate</code> to clear the rate of usage of a resource. Resources that are measured by rate include <code>conns</code>, <code>inspects</code>, and <code>syslogs</code>. You must specify the <code>rate</code> keyword with these resource types. The <code>conns</code> resource is also measured as concurrent connections; only use the <code>rate</code> keyword to view the connections per second. Resources include the following types:</td>
</tr>
<tr>
<td>resource_name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conns</strong>—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hosts</strong>—Hosts that can connect through the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IPSec</strong>—IPSec management tunnels that connect through the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mac-addresses</strong>—The number of MAC addresses allowed in the MAC address table.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Routes</strong>—Routing table entries.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SSH</strong>—SSH sessions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Storage</strong>—Storage limit size of directory in MB.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Telnet</strong>—Telnet sessions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VPN</strong>—VPN resources.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Xlates</strong>—NAT translations.</td>
</tr>
</tbody>
</table>

### Command Default

The default resource name is `all`, which clears all resource types.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example clears the system-wide usage statistics:

```
> clear resource usage resource all
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show resource types</td>
<td>Shows a list of resource types.</td>
</tr>
<tr>
<td>show resource usage</td>
<td>Shows the resource usage of the device.</td>
</tr>
</tbody>
</table>
clear route

To remove dynamically learned routes from the configuration, use the `clear route` command.

```
clear route { all | ip_address mask_or_prefix }
```

**Syntax Description**
- `all`: Specifies that all learned routes are to be removed.
- `ip_address mask_or_prefix`: The IPv4 or IPv6 destination address and mask or prefix of the route to be removed.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to remove all dynamically learned routes.

```
> clear route all
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show route</td>
<td>Displays route information.</td>
</tr>
</tbody>
</table>
clear rule hits

To clear rule hit information for all evaluated rules of access control policies and prefilter policies and reset them to zero, use the `clear rule hits` command.

```
clear rule hits [id]
```

**Syntax Description**

- `id` (Optional) The ID of a rule. Including this argument clears the rule hit information only of the specified rule.
  
  Use the `show access-list` command to identify a rule ID.

**Command Default**

If you do not specify a rule ID, the rule hit information for all the rules are cleared and reset to zero.

**Note**

Exercise caution while using this command as the action is irreversible.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The rule hit information covers only the access control rules and prefilter rules.

**Examples**

Following is an example of clearing all rule hit information:

```
> clear rule hits
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show rule hits</code></td>
<td>Displays the rule hit information for all evaluated rules of access control policies and prefilter policies.</td>
</tr>
<tr>
<td><code>show cluster rule hits</code></td>
<td>Display rule hit information for all evaluated rules of access control policies and prefilter policies from all nodes of a cluster in an aggregated format.</td>
</tr>
<tr>
<td><code>cluster exec show rule hits</code></td>
<td>Display rule hit information for all evaluated rules of access control policies and prefilter policies from each node of a cluster in a segregated format.</td>
</tr>
<tr>
<td><code>cluster exec clear rule hits</code></td>
<td>Clears rule hit information for all evaluated rules of access control policies and prefilter policies and reset them to zero, from all nodes in a cluster.</td>
</tr>
</tbody>
</table>
clear service-policy

To clear operational data or statistics for enabled policies, use the `clear service-policy` command.

`clear service-policy [global | interface intf | shape | user-statistics]`

**Syntax Description**

- **global** (Optional) Clears the statistics of the global service policy.
- **interface intf** (Optional) Clears the service policy statistics of a specific interface.
- **shape** (Optional) Clears the statistics of the shape policy.
- **user-statistics** (Optional) Clears the global counters for user statistics but does not clear the per-user statistics. This feature is not supported by Firepower Threat Defense.

**Command Default**

By default, this command clears all the statistics for all enabled service policies.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Some inspection engines let you selectively clear statistics. See the `clear service-policy inspect` commands.

**Examples**

The following example shows how to clear service policy statistics for the outside interface.

```
> clear service-policy interface outside
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear service-policy inspect</td>
<td>Clears service policy statistics for the GTP, M3UA, and RADIUS inspection engines.</td>
</tr>
<tr>
<td>show service-policy</td>
<td>Displays the service policy.</td>
</tr>
<tr>
<td>show running-config service-policy</td>
<td>Displays the service policies configured in the running configuration.</td>
</tr>
</tbody>
</table>
clear service-policy inspect gtp

To clear GTP inspection statistics, use the clear service-policy inspect gtp command.

clear service-policy inspect gtp {pdp-context {all | apn ap_name | imsi IMSI_value | ms-addr IP_address | tid tunnel_ID | version version_num} | requests {map name | version version_num} | statistics {IP_address}}

Syntax Description

- **pdp-context {all | apn ap_name | imsi IMSI_value | ms-addr IP_address | tid tunnel_ID | version version_num}**
  - Clears Packet Data Protocol (PDP) or bearer context information. You can specify the contexts to clear using the following keywords:
    - **all**—Clear all contexts.
    - **apn ap_name**—Clear contexts for the specified access point name.
    - **imsi IMSI_value**—Clear contexts for the specified IMSI hexadecimal number.
    - **ms-addr IP_address**—Clear contexts for the specified mobile subscriber (MS) IP address.
    - **tid tunnel_ID**—Clear contexts for the specified GTP tunnel ID, a hexadecimal number.
    - **version version_num**—Clear contexts for the specified GTP version (0-255).

- **requests {map name | version version_num}**
  - Clears GTP requests. You can optionally limit the requests to clear using the following parameters:
    - **map name**—Clears requests associated with the specified GTP inspection policy map.
    - **version version_num**—Clears requests for the specified GTP version (0-255).

- **statistics {IP_address}**
  - Clears GTP statistics for the inspect gtp command. You can clear the statistics for a specific endpoint by specifying the endpoint’s address.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example clears GTP statistics:

> clear service-policy inspect gtp statistics
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show service-policy inspect gtp</code></td>
<td>Displays GTP statistics.</td>
</tr>
</tbody>
</table>
clear service-policy inspect m3ua

To clear M3UA inspection statistics, use the `clear service-policy inspect m3ua` command.

```
clear service-policy inspect m3ua  { drops | endpoint [ip_address] }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>drops</code></td>
<td>Clears M3UA drop statistics.</td>
</tr>
<tr>
<td><code>endpoint [ip_address]</code></td>
<td>Clears M3UA endpoint statistics. You can optionally include the IP address of an endpoint to clear only the statistics for that endpoint.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to clear statistics from M3UA inspection. Use the `show` version of this command to view the statistics.

### Examples

The following example clears M3UA endpoint statistics:

```
> clear service-policy inspect m3ua endpoint
```

### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show service-policy inspect m3ua</code></td>
<td>Displays the M3UA statistics.</td>
</tr>
</tbody>
</table>
clear service-policy inspect radius-accounting

To clear RADIUS accounting users, use the `clear service-policy inspect radius-accounting` command.

```
clear service-policy inspect radius-accounting users { all | ip_address | policy_map }
```

**Syntax Description**
- `all`: Clears all users.
- `ip_address`: Clears a user with this IP address.
- `policy_map`: Clears users associated with this policy map.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears all RADIUS accounting users:

```
> clear service-policy inspect radius-accounting users all
```
clear shun

To disable all the shuns that are currently enabled and clear the shun statistics, use the `clear shun` command.

```
clear shun [statistics]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>statistics</td>
<td>(Optional) Clears the interface counters only.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to disable all the shuns that are currently enabled and clear the shun statistics:

```
> clear shun
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>shun</td>
<td>Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.</td>
</tr>
<tr>
<td>show shun</td>
<td>Displays the shun information.</td>
</tr>
</tbody>
</table>
clear snmp-server statistics

To clear SNMP server statistics (SNMP packet input and output counters), use the clear snmp-server statistics command.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to clear SNMP server statistics:

> clear snmp-server statistics

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp-server statistics</td>
<td>Displays SNMP server configuration information.</td>
</tr>
</tbody>
</table>
clear snort statistics

To clear Snort statistics (packet counters, flow counters, and event counters), use the clear snort statistics command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear Snort statistics:

```
> clear snort statistics
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snort statistics</td>
<td>Displays information about the Snort services configuration.</td>
</tr>
</tbody>
</table>
clear snort tls-offload

To clear Snort statistics related to SSL hardware acceleration (connections, encryption, decryption), use the `clear snort tls-offload` command. Consult Cisco TAC to help you debug your system with this command. This command is available only on the following managed devices, which support SSL hardware acceleration:

- Firepower 2100 with Firepower Threat Defense
- Firepower 4100/9300 with Firepower Threat Defense

For information about TLS crypto acceleration support on Firepower 4100/9300 FTD container instances, see the `FXOS Configuration Guide`.

TLS crypto acceleration is *not* supported on any virtual appliances or on any hardware except the preceding.

`clear snort tls-offload [proxy | tracker]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy</td>
<td>(Optional.) Clears statistics for the proxy only.</td>
</tr>
<tr>
<td>tracker</td>
<td>(Optional.) Clears statistics for the tracker only.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following example shows how to clear statics for the proxy:

> clear snort tls-offload proxy

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snort tls-offload</td>
<td>Show statistics for all Snort processes.</td>
</tr>
<tr>
<td>debug snort tls-offload</td>
<td>Displays error debug messages of all types for all Snort processes.</td>
</tr>
</tbody>
</table>
clear ssl

To clear SSL information for debugging purposes, use the `clear ssl` command.

`clear ssl {cache [all] | errors | mib | objects}`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache [all]</td>
<td>Clears expired sessions in SSL session cache. Add the optional all keyword to clear all sessions and statistics in SSL session cache.</td>
</tr>
<tr>
<td>errors</td>
<td>Clears ssl errors.</td>
</tr>
<tr>
<td>mib</td>
<td>Clears SSL MIB statistics.</td>
</tr>
<tr>
<td>objects</td>
<td>Clears SSL object statistics.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTLS cache is never cleared because it would impact AnyConnect functionality.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows clearing ssl cache and clearing all sessions and statistics in SSL session cache.

> `clear ssl cache`
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
> `clear ssl cache all`
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
clear sunrpc-server active

To clear the pinholes opened by Sun RPC application inspection, use the clear sunrpc-server active command.

clear sunrpc-server active

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the clear sunrpc-server active command to clear the pinholes opened by Sun RPC application inspection that allow service traffic, such as NFS or NIS, to pass through the device.

Examples

The following example shows how to clear the SunRPC services table:

> clear sunrpc-server active

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sunrpc-server active</td>
<td>Displays information about active Sun RPC services.</td>
</tr>
</tbody>
</table>
### clear threat-detection rate

To reset threat detection rate statistics to zero, use the `clear threat-detection rate` command.

```
clear threat-detection rate
```

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>6.3</td>
</tr>
</tbody>
</table>

#### Examples

```
> clear threat-detection rate
>
```

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>show threat-detection rate</td>
</tr>
</tbody>
</table>
clear threat-detection scanning-threat

To remove information on the attackers and targets identified through scanning threat detection, use the `clear threat-detection scanning-threat` command.

```
clear threat-detection scanning-threat [attacker [ip_address [mask]] | target [ip_address [mask]]]
```

**Syntax Description**

- **attacker [ip_address [mask]]** (Optional.) Clears attackers only. You can supply an IP address and optional mask to clear a single attacker.
- **target [ip_address [mask]]** (Optional.) Clears targets only. You can supply an IP address and optional mask to clear a single target.

**Command Default**

All attackers and targets are cleared.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows current scanning threats, then clears them.

```
> show threat-detection scanning-threat
Latest Target Host & Subnet List:
  192.168.1.0
  192.168.1.249
Latest Attacker Host & Subnet List:
  192.168.10.234
  192.168.10.0
  192.168.10.2
  192.168.10.3
  192.168.10.4
  192.168.10.5
  192.168.10.6
  192.168.10.7
  192.168.10.8
  192.168.10.9
> clear threat-detection scanning-threat
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show threat-detection scanning-threat</code></td>
<td>Shows scanning threat attackers and targets.</td>
</tr>
</tbody>
</table>
clear threat-detection shun

If you configure scanning threat detection to automatically shun attackers, you can remove hosts from the automatic shun list using the `clear threat-detection shun` command. Use the `clear shun` command to stop shunning a manually shunned host.

`clear threat-detection shun [ip_address [mask]]`

**Syntax Description**

- `ip_address [mask]` (Optional) Releases a specific IP address from being shunned. The subnet mask is optional.

**Command Default**

All shunned attackers are released.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the shun list, then releases host 10.1.1.6.

```
> show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
> clear threat-detection shun 10.1.1.6
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show threat-detection shun</td>
<td>Shows automatically shunned hosts.</td>
</tr>
</tbody>
</table>
clear threat-detection statistics

To reset threat detection statistics to zero, use the `clear threat-detection statistics` command.

```
clear threat-detection statistics [tcp-intercept]
```

**Syntax Description**

| tcp-intercept | (Optional) Clears TCP Intercept statistics. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears all threat detection statistics.

```
> clear threat-detection statistics
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show threat-detection statistics</td>
<td>Shows threat detection statistics.</td>
</tr>
</tbody>
</table>
clear traffic

To reset the counters for transmit and receive activity, use the clear traffic command.

```
clear traffic
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The clear traffic command resets the counters for transmit and receive activity that is displayed with the show traffic command. The counters indicate the number of packets and bytes moving through each interface since the last clear traffic command was entered or since the device came online. And the number of seconds indicate the duration the device has been online since the last reboot.

**Examples**

The following example shows the clear traffic command:

```
> clear traffic
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show traffic</td>
<td>Displays the counters for transmit and receive activity.</td>
</tr>
</tbody>
</table>
clear vpn-sessiondb statistics

To clear statistics for VPN sessions, use the `clear vpn-sessiondb statistics` command.

```
clear vpn-sessiondb statistics  {all | anyconnect | failover | global | index number | ipaddress
IP_address | l2l   | name  username | ospfv3 | protocol protocol | ra-ikev1-ipsec | ra-ikev2-ipsec | tunnel-group name | vpn-lb | webvpn}
```

**Syntax Description**

- **all**
  Clears statistics for all sessions.

- **anyconnect**
  Clears statistics for AnyConnect VPN client sessions.

- **failover**
  Clears statistics for failover IPsec sessions.

- **global**
  Clears statistics for global session data.

- **index index_number**
  Clears statistics of a single session by index number. The output of the `show vpn-sessiondb detail` command displays index numbers for each session.

- **ipaddress IP_address**
  Clears statistics for sessions of the IP address that you specify.

- **l2l**
  Clears statistics for VPN LAN-to-LAN sessions.

- **protocol protocol**
  Clears statistics for specific protocols. Enter "?" to see the list of protocols.

- **ra-ikev1-ipsec**
  Clears statistics for IPsec IKEv1 sessions.

- **ra-ikev2-ipsec**
  Clears statistics for IPsec IKEv2 sessions.

- **tunnel-group groupname**
  Clears statistics for sessions for the tunnel group (connection profile) that you specify.

- **vpn-lb**
  Clears statistics for VPN load balancing management sessions.

- **webvpn**
  Clears statistics for clientless SSL VPN sessions.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears statistics for all VPN sessions:

```
> clear vpn-sessiondb statistics all
INFO: Number of sessions cleared: 20
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show vpn-sessiondb</td>
<td>Displays information about VPN sessions.</td>
</tr>
</tbody>
</table>
clear wccp

To reset Web Cache Communication Protocol (WCCP) information, use the `clear wccp` command.

```
clear wccp [web-cache | service_number]
```

**Syntax Description**

- `web-cache` Specifies the web-cache service.
- `service-number` A dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to reset the WCCP information for the web-cache service:

```
> clear wccp web-cache
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wccp</code></td>
<td>Displays the WCCP configuration.</td>
</tr>
</tbody>
</table>
clear webvpn statistics

To clear statistics for remote access VPN, use the clear webvpn statistics command.

clear webvpn statistics

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Example

The following example clears remote access VPN statistics:

> clear webvpn statistics

Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show webvpn</td>
<td>Displays information about remote access VPN.</td>
</tr>
</tbody>
</table>
clear xlate

To clear current dynamic NAT translation and connection information, use the clear xlate command.

clear xlate [global ip1 [-ip2] [netmask mask] ] [local ip1 [-ip2] [netmask mask] ] [gport port1 [-port2] ] [lport port1 [-port2] ] [interface if_name] [type type]

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>global ip1 [-ip2]</td>
<td>(Optional) Clears the active translations by global IP address or range of addresses.</td>
</tr>
<tr>
<td>gport port1 [-port2]</td>
<td>(Optional) Clears the active translations by the global port or range of ports.</td>
</tr>
<tr>
<td>interface if_name</td>
<td>(Optional) Displays the active translations by interface.</td>
</tr>
<tr>
<td>local ip1 [-ip2]</td>
<td>(Optional) Clears the active translations by local IP address or range of addresses.</td>
</tr>
<tr>
<td>lport port1 [-port2]</td>
<td>(Optional) Clears the active translations by local port or range of ports.</td>
</tr>
<tr>
<td>netmask mask</td>
<td>(Optional) Specifies the network mask or IPv6 prefix to qualify the global or local IP addresses.</td>
</tr>
</tbody>
</table>
| type type | (Optional) Clears the active translations by type. You can enter one of the following types:  
  • dynamic—Specifies dynamic translations.  
  • portmap—Specifies PAT global translations.  
  • static—Specifies static translations.  
  • twice-nat—Specifies a manual NAT translation. |

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The clear xlate command clears the contents of the translation slots (“xlate” refers to the translation slot). Translation slots can persist after key changes have been made. Always use the clear xlate command after adding, changing, or removing NAT rules.

An xlate describes a NAT or PAT session. These sessions can be viewed with the show xlate detail command.

There are two types of xlates: static and dynamic. A static xlate is a persistent xlate that is created using a static NAT rule. The clear xlate command does not clear static entries. Static xlates can only be removed by removing the static NAT rule from the configuration. If you remove a static rule from the configuration, preexisting connections that use the static rule can still forward traffic. Use the clear local-host or clear conn command to deactivate these connections.

A dynamic xlate is an xlate that is created on demand with traffic processing. The clear xlate command removes dynamic xlates and their associated connections. You can also use the clear local-host or clear conn
command to clear the xlate and associated connections. If you remove a dynamic NAT rule from the configuration, the dynamic xlate and associated connections may remain active. Use the `clear xlate` command to remove these connections.

**Examples**

The following example shows how to clear the current translation and connection slot information:

```plaintext
> clear xlate global
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear local-host</td>
<td>Clears local host network information.</td>
</tr>
<tr>
<td>show conn</td>
<td>Displays all active connections.</td>
</tr>
<tr>
<td>show local-host</td>
<td>Displays the local host network information.</td>
</tr>
<tr>
<td>show xlate</td>
<td>Displays the current translation information.</td>
</tr>
</tbody>
</table>
clf - cz

- cluster disable, on page 147
- cluster enable, on page 148
- cluster exec, on page 149
- cluster exec clear rule hits, on page 151
- cluster exec show rule hits, on page 153
- cluster master unit, on page 155
- cluster remove unit, on page 156
- configure coredump packet-engine, on page 157
- configure disable-https-access, on page 158
- configure disable-ssh-access, on page 159
- configure firewall, on page 160
- configure flow-offload, on page 161
- configure high-availability, on page 162
- configure https-access-list, on page 165
- configure inspection, on page 166
- configure log-events-to-ramdisk, on page 171
- configure manager add, on page 172
- configure manager delete, on page 174
- configure manager local, on page 176
- configure network dns searchdomains, on page 178
- configure network dns servers, on page 179
- configure network hostname, on page 180
- configure network http-proxy, on page 181
- configure network http-proxy-disable, on page 182
- configure network ipv4 delete, on page 183
- configure network ipv4 dhcp, on page 184
- configure network ipv4 dhcp-server-disable, on page 185
- configure network ipv4 dhcp-server-enable, on page 186
- configure network ipv4 manual, on page 187
- configure network ipv6 delete, on page 189
- configure network ipv6 destination-unreachable, on page 190
- configure network ipv6 dhcp, on page 191
- configure network ipv6 echo-reply, on page 192
• configure network ipv6 manual, on page 193
• configure network ipv6 router, on page 195
• configure network management-interface, on page 196
• configure network management-port, on page 198
• configure network static-routes, on page 199
• configure password, on page 201
• configure snort, on page 202
• configure ssh-access-list, on page 203
• configure ssl-protocol, on page 204
• configure tcp-randomization, on page 205
• configure unlock_time, on page 208
• configure user access, on page 209
• configure user add, on page 210
• configure user aging, on page 212
• configure user delete, on page 213
• configure user disable, on page 214
• configure user enable, on page 215
• configure user forcereset, on page 216
• configure user maxfailedlogins, on page 217
• configure user minpasswdlen, on page 218
• configure user password, on page 219
• configure user strengthcheck, on page 220
• configure user unlock, on page 221
• connect fxos, on page 222
• copy, on page 223
• cpu hog granular-detection, on page 226
• cpu profile activate, on page 227
• cpu profile dump, on page 229
• crashinfo force, on page 231
• crashinfo test, on page 232
• crypto ca trustpool export, on page 233
• crypto ca trustpool import, on page 234
• crypto ca trustpool remove, on page 236
cluster disable

To disable clustering on a unit, use the **cluster disable** command.

**cluster disable**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.5</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command lets you manually remove a cluster unit from the cluster.

**Examples**

The following example enables clustering on a unit:

```shell
> cluster disable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster enable</td>
<td>Enables clustering.</td>
</tr>
<tr>
<td>cluster master unit</td>
<td>Sets a new unit as the master unit of a cluster.</td>
</tr>
<tr>
<td>cluster remove unit</td>
<td>Removes the unit from the cluster.</td>
</tr>
<tr>
<td>show cluster info</td>
<td>Shows cluster information.</td>
</tr>
<tr>
<td>cluster exec</td>
<td>Sends a command to all cluster members.</td>
</tr>
</tbody>
</table>
cluster enable

To enable clustering on a unit, use the `cluster enable` command.

```
class enable
```

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the first unit enabled, a master unit election occurs. Because the first unit should be the only member of the cluster so far, it will become the master unit. Do not perform any configuration changes during this period.

**Examples**

The following example enables clustering on a unit:

```
> cluster enable
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>cluster disable</code></td>
<td>Disables clustering.</td>
</tr>
<tr>
<td></td>
<td><code>cluster master unit</code></td>
<td>Sets a new unit as the master unit of a cluster.</td>
</tr>
<tr>
<td></td>
<td><code>cluster remove unit</code></td>
<td>Removes the unit from the cluster.</td>
</tr>
<tr>
<td></td>
<td><code>show cluster info</code></td>
<td>Shows cluster information.</td>
</tr>
<tr>
<td></td>
<td><code>cluster exec</code></td>
<td>Sends a command to all cluster members.</td>
</tr>
</tbody>
</table>
**cluster exec**

To execute a command on all units in the cluster, or on a specific member, use the `cluster exec` command.

```
cluster exec  [unit  unit_name]  command
```

**Syntax Description**

- `unit unit_name` *(Optional)* Performs the command on a specific unit. To view member names, enter `cluster exec unit ?` (to see all names except the current unit), or enter the `show cluster info` command.

- `command` Specifies the command you want to execute.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Sending a `show` command to all members collects all output and displays it on the console of the current unit. Other commands, such as `capture` and `copy`, can also take advantage of cluster-wide execution.

**Examples**

To copy the same capture file from all units in the cluster at the same time to a TFTP server, enter the following command on the master unit:

```
> cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as `capture1_device1.pcap`, `capture1_device2.pcap`, and so on. In this example, `device1` and `device2` are cluster unit names.

The following sample output for the `cluster exec show port-channel summary` command shows EtherChannel information for each member in the cluster:

```
> cluster exec show port-channel summary
primary{LOCAL}:******************************************************************************
Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
-----------------------------------------------
1      Po1          LACP      Yes  Gi0/0(P)
2      Po2          LACP      Yes  Gi0/1(P)
secondary:******************************************************************************
Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
-----------------------------------------------
1      Po1          LACP      Yes  Gi0/0(P)
2      Po2          LACP      Yes  Gi0/1(P)
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster enable</td>
<td>Enables clustering on a unit.</td>
</tr>
<tr>
<td>cluster master unit</td>
<td>Sets a new unit as the master unit of a cluster.</td>
</tr>
<tr>
<td>cluster remove unit</td>
<td>Removes the unit from the cluster.</td>
</tr>
<tr>
<td>show cluster info</td>
<td>Shows cluster information.</td>
</tr>
<tr>
<td>cluster exec</td>
<td>Sends a command to all cluster members.</td>
</tr>
</tbody>
</table>
cluster exec clear rule hits

To clear rule hit information for all evaluated rules of access control policies and prefilter policies and reset them to zero, from all nodes in a cluster, use the `cluster exec clear rule hits` command.

**Syntax Description**

```
cluster exec clear rule hits  [id]
```

- **id** (Optional) The ID of a rule. Including this argument clears the rule hit information only of the specified rule.

Use the `show access-list` command to identify a rule ID. However, not all the rules are listed in the output of this command. You can trigger a REST API GET operation on the following URLs to see all the rules and their IDs:

- `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`
- `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`

**Command Default**

If you do not specify a rule ID, the rule hit information for all the rules are cleared and reset to zero.

**Note**

Exercise caution while using this command as the action is irreversible.

**Command History**

**Release**  **Modification**

6.4  This command was introduced.

**Usage Guidelines**

The rule hit information covers only the access control rules and prefilter rules.

**Examples**

Following is an example of clearing all rule hit information:

```
> cluster exec clear rule hits
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cluster rule hits</code></td>
<td>Display rule hit information for all evaluated rules of access control policies and prefilter policies from all nodes of a cluster in an aggregated format.</td>
</tr>
<tr>
<td><code>cluster exec show rule hits</code></td>
<td>Display rule hit information for all evaluated rules of access control policies and prefilter policies from each node of a cluster in a segregated format.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>show rule hits</strong></td>
<td>Displays the rule hit information for all evaluated rules of access control policies and prefilter policies.</td>
</tr>
<tr>
<td><strong>clear rule hits</strong></td>
<td>Clears the rule hit information for all evaluated rules of access control policies and prefilter policies and resets them to zero.</td>
</tr>
</tbody>
</table>
**cluster exec show rule hits**

To display rule hit information for all evaluated rules of access control policies and prefilter policies, from each node of a cluster in a segregated format, use the `cluster exec show rule hits` command.

```bash
cluster exec show rule hits [id | raw | gt #hit-count | lt #hit-count | range #hit-count1 #hit-count2]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>(Optional) The ID of a rule. Including this argument limits the displayed information to the specified rule. Use the <code>show access-list</code> command to identify a rule ID. However, not all the rules are listed in the output of this command. You can trigger a REST API GET operation on the following URLs to see all the rules and their IDs:</td>
</tr>
<tr>
<td></td>
<td><img src="null" alt="URLs" /></td>
</tr>
<tr>
<td>raw</td>
<td>(Optional) Displays the rule hit information in .csv format.</td>
</tr>
<tr>
<td>gt #hit-count</td>
<td>(Optional) Displays all the rules that have a hit count greater than #hit-count.</td>
</tr>
<tr>
<td>lt #hit-count</td>
<td>(Optional) Displays all the rules that have a hit count lesser than #hit-count.</td>
</tr>
<tr>
<td>range #hit-count1</td>
<td>(Optional) Displays all the rules that have a hit count in-between #hit-count1 and #hit-count2.</td>
</tr>
</tbody>
</table>

**Command Default**

If you do not specify a rule ID, the rule hit information for all the rules are shown.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The rule hit information covers only the access control rules and prefilter rules.

**Examples**

The following example displays rule hit information from each node of a cluster in a segregated format:

```bash
> cluster exec show rule hits
unit-1-1(LOCAL):******************************************************************************

<table>
<thead>
<tr>
<th>RuleID</th>
<th>Hit Count</th>
<th>First Hit Time(UTC)</th>
<th>Last Hit Time(UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>268435261</td>
<td>1</td>
<td>06:55:19 Mar 8 2019</td>
<td>06:55:19 Mar 8 2019</td>
</tr>
</tbody>
</table>
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cluster exec clear rule hits</strong></td>
<td>Clears rule hit information for all evaluated rules of access control policies and prefilter policies and reset them to zero, from all nodes in a cluster.</td>
</tr>
<tr>
<td><strong>show cluster rule hits</strong></td>
<td>Display rule hit information for all evaluated rules of access control policies and prefilter policies from all nodes of a cluster in an aggregated format.</td>
</tr>
<tr>
<td><strong>show rule hits</strong></td>
<td>Displays the rule hit information for all evaluated rules of access control policies and prefilter policies.</td>
</tr>
<tr>
<td><strong>clear rule hits</strong></td>
<td>Clears the rule hit information for all evaluated rules of access control policies and prefilter policies and resets them to zero.</td>
</tr>
</tbody>
</table>
cluster master unit

To set a new unit as the master unit of a device cluster, use the **cluster master unit** command.

```
cluster master unit unit_name
```

### Syntax Description

| **unit_name** | Specifies the local unit name to be the new master unit. To view member names, enter `cluster master unit ?` (to see all names except the current unit), or enter the `show cluster info` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You will need to reconnect to the main cluster IP address.

### Examples

The following example sets **device2** as the master:

```
> cluster master unit device2
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster enable</td>
<td>Enables clustering on a unit.</td>
</tr>
<tr>
<td>cluster exec</td>
<td>Sends a command to all cluster members.</td>
</tr>
<tr>
<td>cluster remove unit</td>
<td>Removes the unit from the cluster.</td>
</tr>
<tr>
<td>show cluster info</td>
<td>Shows cluster information.</td>
</tr>
</tbody>
</table>
cluster remove unit

To remove the unit from the cluster, use the `cluster remove unit` command.

```
cluster remove unit  unit_name
```

**Syntax Description**

| unit_name | Specifies the local unit name to remove from the cluster. To view member names, enter `cluster remove unit ?`, or enter the `show cluster info` command. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The bootstrap configuration remains intact, as well as the last configuration synced from the master unit, so you can later re-add the unit without losing your configuration. If you enter this command on a slave unit to remove the master unit, a new master unit is elected.

**Examples**

The following example checks for unit names, and then removes device2 from the cluster:

```
> cluster remove unit ?
Current active units in the cluster:
device2
> cluster remove unit device2
WARNING: Clustering will be disabled on unit device2. To bring it back to the cluster please logon to that unit and re-enable clustering
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster enable</td>
<td>Enables clustering on a unit.</td>
</tr>
<tr>
<td>cluster exec</td>
<td>Sends a command to all cluster members.</td>
</tr>
<tr>
<td>cluster master unit</td>
<td>Sets a new unit as the master unit of a cluster.</td>
</tr>
<tr>
<td>show cluster info</td>
<td>Shows cluster information.</td>
</tr>
</tbody>
</table>
configure coredump packet-engine

To enable or disable packet-engine coredump generation, use the configure coredump packet-engine command.

configure coredump packet-engine  {enable | disable}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables the packet-engine coredump generation.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables the packet-engine coredump generation.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Packet-engine coredump generation is enabled by default.

This command is only available on the Firepower 2100 series. When you run this command on an unsupported platform, the system returns the following message:

This command is not available on this platform.

Examples

The following example disables packet-engine coredump generation.

> configure coredump packet-engine disable

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show coredump</td>
<td>Displays the packet-engine coredump generation settings.</td>
</tr>
</tbody>
</table>
**configure disable-https-access**

To clear the HTTPS access list, configuring the device to reject HTTPS connection attempts from all IP addresses, use the `configure disable-https-access` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to disable HTTPS access to the device. HTTPS access is required when using the local manager, Firepower Device Manager.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

**Examples**

The following example configures the device to reject HTTPS connections from any address:

```
> configure disable-https-access
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure https-access-list</code></td>
<td>Configures the device to accept HTTPS connections from specified IP addresses.</td>
</tr>
<tr>
<td><code>show https-access-list</code></td>
<td>Shows the current HTTPS access list.</td>
</tr>
</tbody>
</table>
configure disable-ssh-access

To clear the SSH access list, configuring the device to reject SSH connection attempts from all IP addresses, use the `configure disable-ssh-access` command.

```
configure disable-ssh-access
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to disable SSH access to the device. This prevents CLI access except through the Console port.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

### Examples

The following example configures the device to reject SSH connections from any address:

```
> configure disable-ssh-access
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure ssh-access-list</code></td>
<td>Configures the device to accept SSH connections from specified IP addresses.</td>
</tr>
<tr>
<td><code>show ssh-access-list</code></td>
<td>Shows the current SSH access list.</td>
</tr>
</tbody>
</table>
**configure firewall**

To set the firewall mode to transparent or routed mode, use the `configure firewall` command.

```
configure firewall { routed | transparent }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routed</td>
<td>Sets the firewall mode to routed firewall mode.</td>
</tr>
<tr>
<td>transparent</td>
<td>Sets the firewall mode to transparent firewall.</td>
</tr>
</tbody>
</table>

**Command Default**

By default, the device is in routed mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A transparent firewall is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

When you change modes, the device clears the configuration because many commands are not supported for both modes. If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration.

**Note**

You cannot switch to transparent firewall mode if you are using the local device manager, Firepower Device Manager. If you are using the local manager and you want to convert to transparent mode, you must first use `configure manager delete` to remove the manager, convert to transparent mode, then use `configure manager add` to point to a Firepower Management Center.

**Examples**

The following example changes the firewall mode to transparent:

```
configure firewall transparent
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Shows the running configuration.</td>
</tr>
<tr>
<td>show firewall</td>
<td>Shows the firewall mode.</td>
</tr>
</tbody>
</table>
configure flow-offload

This command enables or disables accelerating certain flows (that is, traffic) by processing them in hardware. Offloading flow processing to hardware increases performance, and is enabled by default.

Dynamic flow offload is supported on a Firepower Threat Defense on the Firepower 4100/9300 chassis. Dynamic flow offload enables you to select traffic to be offloaded to hardware, which means it is not processed by the software or CPU of your Firepower Threat Defense device.

configure flow-offload dynamic whitelist {enable | disable}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic whitelist enable</td>
<td>Enable dynamic offload.</td>
</tr>
<tr>
<td>dynamic whitelist disable</td>
<td>Disable dynamic offload.</td>
</tr>
</tbody>
</table>

Command Default

Enabled by default.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

For information about dynamic flow offload support and limitations, see the chapter on common rule characteristics in the Firepower Management Center Configuration Guide.

Examples

Following is an example of disabling dynamic offload:

> configure flow-offload dynamic whitelist disable

Following is an example of enabling dynamic offload:

> configure flow-offload dynamic whitelist enable

Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show flow-offload</td>
<td>Displays dynamic flow offload counters, statistics, and information.</td>
</tr>
<tr>
<td>clear flow-offload</td>
<td>Clears dynamic flow offload flows, counters, or statistics.</td>
</tr>
</tbody>
</table>
**configure high-availability**

To disable, suspend, or resume a high-availability configuration (failover) between devices, use the `configure high-availability` command.

```
configure high-availability { disable [clear-interfaces] | resume | suspend [clear-interfaces] }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>clear-interfaces (Optional) Clears interface configurations upon disabling or suspending high availability.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Breaks the high-availability relationship between this device and its peer. You cannot use this option on a locally-managed device; use FDM instead. If you mistakenly use the disable command, you must follow it with an FTD API call using the BreakHAStatus resource to complete the action.</td>
</tr>
<tr>
<td>resume</td>
<td>Resumes a temporarily suspended high-availability configuration between this device and its peer. The unit will negotiate active/standby status with the peer unit. You cannot resume a disabled configuration.</td>
</tr>
<tr>
<td>suspend</td>
<td>Temporarily suspends a high-availability configuration between this device and its peer. You can later resume the configuration. If you suspend high availability from the active unit, the configuration is suspended on both the active and standby unit. If you suspend it from the standby unit, it is suspended on the standby unit only, but the active unit will not attempt to failover to a suspended unit.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can configure two devices as a high-availability pair. This is also known as a failover configuration, where one device can take over if the other device in the pair fails.

You can use the `configure high-availability` command to manage the high-availability pair if for some reason you cannot update the configuration in the device manager. For example, if you cannot reach the high availability pair, you can use `configure high-availability disable` to remove the failover configuration from both high availability peers.

You can also temporarily suspend the failover configuration, then resume it later. Suspending HA on a unit is useful when:

- Both units are in an active-active situation and fixing the communication on the failover link does not correct the problem.
- You want to troubleshoot an active or standby unit and do not want the units to fail over during that time.
- You want to prevent failover while installing a software upgrade on the standby device.

When you suspend high availability, you stop the pair of devices from behaving as a failover unit. The currently active device remains active, handling all user connections. However, failover criteria are no longer monitored,
and the system will never fail over to the now pseudo-standby device. The standby device will retain its configuration, but it will remain inactive.

The key difference between suspending HA and breaking HA is that on a suspended HA device, the high availability configuration is retained. When you break HA, the configuration is erased. Thus, you have the option to resume HA on a suspended system, which enables the existing configuration and makes the two devices function as a failover pair again.

Note

Suspending high availability is a temporary state. If you reload a unit, it resumes the high-availability configuration automatically and negotiates the active/standby state with the peer.

Examples

The following example shows how to temporarily suspend and then resume a high-availability configuration.

```plaintext
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MPF0H1CP
  This host: Primary - Active
    Active time: 776671 (sec)
    slot 0: empty
      Interface outside (192.168.77.1): Normal (Waiting)
      Interface inside (192.168.87.1): Normal (Waiting)
      Interface diagnostic (0.0.0.0): Normal (Waiting)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)
  Other host: Secondary - Standby Ready
    Active time: 53 (sec)
    Interface outside (0.0.0.0): Normal (Waiting)
    Interface inside (0.0.0.0): Normal (Waiting)
    Interface diagnostic (0.0.0.0): Normal (Waiting)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)
(...Output truncated...)
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to abort: Yes
Successfully suspended high-availability.
> show failover
Failover Off
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
```
configure high-availability

Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http

> configure high-availability resume
Successfully resumed high-availability.

> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http

Unit Enrollment Hold action is active, timeout in 1792 seconds
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate Unknown
Last Failover at: 20:26:06 UTC Nov 4 2016

This host: Primary - Active
Active time: 778071 (sec)
  slot 0: empty
  Interface outside (192.168.77.1): Normal (Waiting)
  Interface inside (192.168.87.1): Normal (Waiting)
  Interface diagnostic (0.0.0.0): Normal (Waiting)
  slot 1: snort rev (1.0) status (up)
  slot 2: diskstatus rev (1.0) status (up)

Other host: Secondary - App Sync
Active time: 53 (sec)
  Interface outside (0.0.0.0): Unknown (Waiting)
  Interface inside (0.0.0.0): Unknown (Waiting)
  Interface diagnostic (0.0.0.0): Unknown (Waiting)
  slot 1: snort rev (1.0) status (up)
  slot 2: diskstatus rev (1.0) status (up)

(...Output truncated...)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show failover</td>
<td>Shows the failover (high-availability) configuration.</td>
</tr>
<tr>
<td>show high-availability config</td>
<td>Shows the failover (high-availability) configuration. Provides the same output as show failover.</td>
</tr>
</tbody>
</table>
**configure https-access-list**

To configure the device to accept HTTPS connections from specified IP addresses, use the `configure https-access-list` command.

```
configure https-access-list address_list
```

**Syntax Description**

| address_list | A comma separated list of IP addresses for hosts or networks, in IPv4 Classless Inter-Domain Routing (CIDR) notation or IPv6 prefix length notation. For example, 10.100.10.0/24 or 2001:DB8::/96. To specify all IPv4 hosts, enter 0.0.0.0/0. To specify all IPv6 hosts, specify ::/0. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must include all supported hosts or networks in a single command. Addresses specified in this command overwrite the current contents of the HTTPS access list.

Merely allowing HTTPS access does not permit users to log into the local manager. Access to the configuration software is controlled by username and password.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

**Examples**

The following example configures the device to accept HTTPS connections from any IPv4 or IPv6 address:

```
> configure https-access-list 0.0.0.0/0,::/0
The https access list was changed successfully.
> show https-access-list
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:https
ACCEPT tcp anywhere anywhere state NEW tcp dpt:https
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure disable-https-access</td>
<td>Clears the HTTPS access list.</td>
</tr>
<tr>
<td>show https-access-list</td>
<td>Shows the HTTPS access list.</td>
</tr>
</tbody>
</table>
**configure inspection**

To enable or disable the default application protocol inspection engines, use the `configure inspection` command.

```
configure inspection protocol {enable | disable}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>disable</code></td>
<td>Disables the inspection engine.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables the inspection engine.</td>
</tr>
<tr>
<td><code>protocol</code></td>
<td>The inspection protocol that you want to enable or disable. See the usage guidelines section for a list of options.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Although you can disable inspections when using Firepower Device Manager, each time you deploy the configuration from Firepower Device Manager, the default inspections are re-enabled. If you want to keep an inspection disabled, you must re-enter the command after each deployment. Starting with version 6.2.3, you can enable and disable these inspections using FlexConfig to make changes that persist.

Disable the default inspection engines only at the direction of Cisco Technical Support, or if you are certain that the associated types of traffic do not occur on your network. For example, if you block all traffic on an inspected port, you can safely disable inspection on that port. These inspections are applied to all data interfaces.

These inspection engines are separate from Snort inspection. These engines provide the following services:

- **Pinhole creation**—Some application protocols open secondary TCP or UDP connections either on standard or negotiated ports. Inspection opens pinholes for these secondary ports so that you do not need to create access control rules to allow them.

- **NAT rewrite**—Protocols such as FTP embed IP addresses and ports for the secondary connections in packet data as part of the protocol. If there is NAT translation involved for either of the endpoints, the inspection engines rewrite the packet data to reflect the NAT translation of the embedded addresses and ports. The secondary connections would not work without NAT rewrite. For NAT limitations, see the NAT chapter in the configuration guide for the manager you are using to configure the device (Firepower Management Center or Firepower Device Manager).

- **Protocol enforcement**—Some inspections enforce some degree of conformance to the RFCs for the inspected protocol.

You can disable, and subsequently enable, the following inspection engines. To see what is currently enabled, use the `show running-config policy-map` command and look for the `inspect` commands. To see details of the default parameters for each inspection, use the `show running-config all policy-map` command.
• **dcerpc**—(TCP port 135.) Distributed Computing Environment/Remote Procedure Calls. The DCERPC inspection engine inspects for native TCP communication between the Endpoint Mapper (EPM) and client on well known TCP port 135. Microsoft Remote Procedure Call (MSRPC), based on DCERPC, is a protocol widely used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely. Inspection provides pinhole creation and NAT services.

• **dns**—(UDP port 53.) Domain Name System. DNS is inspected on UDP port 53. Inspection provides NAT services and protocol enforcement. You must enable this inspection engine to use the NAT rewrite option on NAT rules. NAT rewrite is frequently required when doing NAT between IPv4 and IPv6 networks (NAT64/46).

• **esmtp**—(TCP port 25.) Extended Simple Mail Transfer Protocol. ESMTP inspection detects attacks, including spam, phishing, malformed message attacks, and buffer overflow/underflow attacks. It also provides support for application security and protocol conformance, which enforces the sanity of the ESMTP messages as well as block senders/receivers, and block mail relay. For details on the controls applied during inspection, use the `show running-config all policy-map` command and look for the “policy-map type inspect esmtp_default_esmtp_map” line and subsequent parameters.

ESMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns. It provides NAT services and protocol conformance. ESMTP inspection performs three primary tasks:

- Restricts SMTP requests to seven basic SMTP commands and eight extended commands. Supported commands are the following:
  
  Extended SMTP—AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML, STARTTLS, and VRFY.
  
  SMTP (RFC 821)—DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET.

- Monitors the SMTP command-response sequence.

- Generates an audit trail. Syslog audit record 108002 is generated when an invalid character embedded in the mail address is replaced. For more information, see RFC 821.

• **ftp**—(TCP port 21.) File Transfer Protocol. Inspection provides pinhole and NAT services.

• **h323_h225**—(TCP port 1720, UDP port 1718.) H.323 inspection supports RAS, H.225, and H.245, and its functionality translates all embedded IP addresses and ports. It performs state tracking and filtering. H.323 inspection provides support for H.323 compliant applications such as Cisco CallManager. H.323 is a suite of protocols defined by the International Telecommunication Union for multimedia conferences over LANs. The device supports H.323 through Version 6, including H.323 v3 feature Multiple Calls on One Call Signaling Channel.

The two major functions of H.323 inspection are as follows:

- NAT the necessary embedded IPv4 addresses in the H.225 and H.245 messages. Because H.323 messages are encoded in PER encoding format, the ASA uses an ASN.1 decoder to decode the H.323 messages.

- Dynamically allocate the negotiated H.245 and RTP/RTCP connections. The H.225 connection can also be dynamically allocated when using RAS.

• **h323_ras**—(UDP ports 1718-1719.) See the description for **h323_h225**. This inspection is for RAS signaling.

• **icmp**—(ICMP traffic only.) The ICMP inspection engine allows ICMP traffic to have a “session” so it can be inspected like TCP and UDP traffic. Without the ICMP inspection engine, we recommend that
you do not allow ICMP through the device (block with an access control rule). Without stateful inspection, ICMP can be used to attack your network. The ICMP inspection engine ensures that there is only one response for each request, and that the sequence number is correct. Inspection also provides NAT services.

- **icmp_error**—(ICMP traffic only.) When ICMP Error inspection is enabled, the device creates translation sessions for intermediate hops that send ICMP error messages, based on the NAT configuration. The device overwrites the packet with the translated IP addresses. This is necessary to provide meaningful information in traceroutes that go through the device.

- **ip-options**—(RSVP traffic only.) IP Options inspection controls which IP packets are allowed based on the contents of the IP Options field in the packet header. Packets with the Router Alert option are allowed. Packets with any other options are dropped.

- **netbios**—(UDP source ports 137, 138.) NetBIOS Name Server over IP. NetBIOS application inspection performs NAT for the embedded IP address in the NetBIOS name service (NBNS) packets and NetBIOS datagram services packets. It also enforces protocol conformance, checking the various count and length fields for consistency.

- **rsh**—(TCP port 514.) The RSH protocol uses a TCP connection from the RSH client to the RSH server on TCP port 514. The client and server negotiate the TCP port number where the client listens for the STDERR output stream. RSH inspection opens pinholes and supports NAT of the negotiated port number if necessary.

- **rtsp**—(TCP port 554.) Real-Time Streaming Protocol. The RTSP inspection engine lets the device pass RTSP packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime, RealPlayer, and Cisco IP/TV connections. RTSP applications use the well-known port 554 with TCP (rarely UDP) as a control channel. The device only supports TCP, in conformity with RFC 2326. This TCP control channel is used to negotiate the data channels that are used to transmit audio/video traffic, depending on the transport mode that is configured on the client. The supported RDT transports are: rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp, and x-pn-tng/udp.

- **sqlnet**—(TCP port 1521.) The inspection engine supports SQL*Net versions 1 and 2, but only the Transparent Network Substrate (TNS) format. Inspection does not support the Tabular Data Stream (TDS) format. SQL*Net messages are scanned for embedded addresses and ports, and NAT rewrite is applied when necessary.

  Disable SQL*Net inspection when SQL data transfer occurs on the same port as the SQL control TCP port 1521. The security appliance acts as a proxy when SQL*Net inspection is enabled and reduces the client window size from 65000 to about 16000 causing data transfer issues.

- **sip**—(TCP/UDP port 5060.) Session Initiation Protocol. SIP is a widely used protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. Partially because of its text-based nature and partially because of its flexibility, SIP networks are subject to a large number of security threats. SIP application inspection provides address translation in message header and body, dynamic opening of ports and basic sanity checks.

- **skinny**—(TCP port 2000.) Skinny Client Control Protocol (SCCP). SCCP (Skinny) application inspection performs translation of embedded IP address and port numbers within the packet data, and dynamic opening of pinholes. It also performs additional protocol conformance checks and basic state tracking.

- **sunrpe**—(TCP/UDP port 111.) Sun RPC is used by NFS and NIS. Sun RPC services can run on any port. When a client attempts to access a Sun RPC service on a server, it must learn the port that service is running on. It does this by querying the port mapper process, usually rpcbind, on the well-known port of 111.
The client sends the Sun RPC program number of the service and the port mapper process responds with the port number of the service. The client sends its Sun RPC queries to the server, specifying the port identified by the port mapper process. When the server replies, the device intercepts this packet and opens both embryonic TCP and UDP connections on that port. NAT or PAT of Sun RPC payload information is not supported.

- **tftp**—(UDP port 69.) Trivial File Transfer Protocol. The inspection engine inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR), and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server.

  A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid read (RRQ) or write (WRQ) request. This secondary channel is subsequently used by TFTP for file transfer or error notification. Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel. TFTP inspection must be enabled if static PAT is used to redirect TFTP traffic.

- **xdmcp**—(UDP port 177.) X Display Manager Control Protocol. XDMCP is a protocol that uses UDP port 177 to negotiate X sessions, which use TCP when established. For successful negotiation and start of an XWindows session, the device must allow the TCP back connection from the Xhosted computer. Use access control rules to permit the back connection through the TCP ports.

  During the XWindows session, the manager talks to the display Xserver on the well-known port 6000 | n. Each display has a separate connection to the Xserver, as a result of the following terminal setting:

  ```
  setenv DISPLAY Xserver:n, where n is the display number.
  ```

  When XDMCP is used, the display is negotiated using IP addresses, which the device can NAT if needed. XDCMP inspection does not support PAT.

**Examples**

The following example shows the current inspection configuration and disables XDMCP inspection. You can enable or disable inspection engines, but you cannot change their default behavior. For example, this output shows that DNS/TCP inspection is disabled. You cannot configure DNS inspection to apply to TCP traffic using the `configure inspection` command.

```bash
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
  parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
  class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect smtp
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
```
configure inspection

inspect netbios
inspect tftp
inspect ip-options
inspect icmp
inspect icmp error
inspect dcerpc

configure inspection xdmcp disable

Building configuration...
Cryptochecksum: 46dbea1d 51c2089a fcc3e42f 3dafd2d5
12386 bytes copied in 0.160 secs
[OK]

show running-config policy-map

policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rsvp
inspect esmtp
inspect smtp
inspect skinny
inspect sqlnet
inspect skinny
inspect sunrpc
inspect sip
inspect netbios
inspect tftp
inspect ip-options
inspect icmp
inspect icmp error
inspect dcerpc
inspect ftp

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config policy-map</td>
<td>Shows the policy maps for service policies, including the inspection configuration.</td>
</tr>
<tr>
<td>show service-policy</td>
<td>Shows service-policy statistics, including those for inspection.</td>
</tr>
</tbody>
</table>
configure log-events-to-ramdisk

To enable or disable connection event logging to RAM disk to improve system performance and reduce disk
wear associated with writing connection events to the Solid State Drive (SSD), use the configure
log-events-to-ramdisk command.

configure log-events-to-ramdisk { enable | disable }

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables connection event logging to RAM disk.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables connection event logging to RAM disk. Connection events are then logged to the SSD.</td>
</tr>
</tbody>
</table>

Command Default

The default is enabled on the platforms that support the feature.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to toggle between using RAM disk or a physical SSD to log connection events. If enabled,
connection events are logged to RAM disk. If disabled, connection events are logged to the SSD. In the event
of a power loss, connection events logged to RAM disk will be lost.

This command is only available on the ASA 5512, ASA 5515, and the Firepower 4100 series. When you run
this command on an unsupported platform, the system returns the following message:

This command is not available on this platform.

Examples

The following example disables RAM disk logging.

> configure log-events-to-ramdisk disable

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show log-events-to-disk</td>
<td>Display the current logging status.</td>
</tr>
<tr>
<td>show disk-manager</td>
<td>Displays detailed disk usage information for each part of the system, including silos, low watermarks, and high watermarks.</td>
</tr>
</tbody>
</table>
configure manager add

To configure the device to accept a connection from or initiate a connection to a Firepower Management Center, use the `configure manager add` command.

⚠️ Caution

Adding a remote manager resets the configuration to the factory default.

configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id]

**Syntax Description**

- **hostname**: Specifies the hostname of the FMC.
- **IPv4_address**: Specifies the IPv4 address of the FMC.
- **IPv6_address**: Specifies the IPv6 address of the FMC.
- **DONTRESOLVE**: If the FMC is not directly addressable, use `DONTRESOLVE`. If you use `DONTRESOLVE`, then a `nat_id` is required. When you add this device to the FMC, make sure that you specify both the device IP address and the `nat_id`; one side of the connection needs to specify an IP address, and both sides need to specify the same, unique NAT ID.
- **regkey**: Specifies the unique alphanumeric registration key required to register a device to the FMC.
- **nat_id**: Specifies an alphanumeric string used during the registration process between the FMC and the device when one side does not specify an IP address. Specify the same NAT ID on the FMC.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A unique alphanumeric registration key is always required to register a device to a FMC.

Normally, you need both IP addresses: the Firepower Management Center specifies the device IP address, and the device specifies the Firepower Management Center IP address. However, if you only know one of the IP addresses, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. If you do not know the Firepower Management Center IP address, then use the `DONTRESOLVE` keyword instead of the IP address or hostname.

If you registered a Firepower Management Center and a device using IPv4 and want to convert them to IPv6, you must delete and re-register the device on the Firepower Management Center.

To change from FMC to the local Firepower Device Manager, use the `configure manager delete` command, and then use the `configure manager local` command.
Before moving a device from one FMC to another or changing to the local manager, delete it from the current FMC.

**Examples**

```bash
> configure manager add DONTRESOLVE abc123 efg456
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure manager delete</td>
<td>Removes the managing Firepower Management Center.</td>
</tr>
<tr>
<td>configure manager local</td>
<td>Configures the local manager.</td>
</tr>
<tr>
<td>show managers</td>
<td>Shows the current manager.</td>
</tr>
</tbody>
</table>
configure manager delete

To disable the current manager and enter No Manager Mode, use the `configure manager delete` command.

⚠️ Caution
Deleting the manager resets the FTD configuration to the factory default. However, the management bootstrap configuration is maintained.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.3</td>
<td>The check for high availability mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to remove the current device manager. The device is placed in No Manager Mode, where you can then either add a remote manager (Firepower Management Center) or use the local manager (Firepower Device Manager). You would use this command when switching between local and remote management, or when a remote manager is no longer active.

If the device is configured for high availability, you must first break the high availability configuration using the device manager (if possible) or the `configure high-availability disable` command. Ideally, break HA from the active unit.

The command behavior differs based on the current manager.

- Remote—The Firepower Management Center cannot be reachable. If the FMC is still communicating with the FTD, first remove the device from the FMC’s inventory. Then you can use this command.
- Local—No restrictions. You are immediately moved to No Manager Mode.

**Examples**

The following example removes the current manager and enters No Manager Mode.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in Firepower Device Manager before deleting the local manager. Otherwise, those licenses remain assigned to the device in Cisco Smart Software Manager.
Do you want to continue[yes/no]: yes
DHCP Server Disabled
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure manager add</td>
<td>Configures a managing Firepower Management Center for the device.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>configure manager local</td>
<td>Configures a local manager.</td>
</tr>
<tr>
<td>show managers</td>
<td>Shows the current manager.</td>
</tr>
</tbody>
</table>
configure manager local

To configure the device to use the local manager, Firepower Device Manager, use the `configure manager local` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to enable the local manager, Firepower Device Manager. Use the local manager when you do not want to use a separate Firepower Management Center. By enabling the local manager, you can open Firepower Device Manager using a browser at `http://management_ip_address`.

The local manager is available for the following platforms only:

- ASA 5506-X (all variations), 5508-X, 5516-X.
- Firepower 2100 series.
- Firepower Threat Defense Virtual
- ISA 3000 (Cisco 3000 Series Industrial Security Appliances)

For all other platforms, configure a remote manager using the `configure manager add` command.

### Note

It can take up to 4-6 minutes for the command to complete, because the system must reinitialize its database. Please be patient.

### Additional Restrictions

- The device must be in No Manager Mode before you can switch to the local manager. Use the `configure manager delete` command to enter No Manager Mode. Use the `show managers` command to determine your current manager.
- The device cannot be operating in transparent firewall mode (see the `configure firewall` command). The local manager supports routed mode only.

### Examples

The following example shows how to configure the local manager.

```
> configure manager local
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure manager add</td>
<td>Configures a managing Firepower Management Center for the device.</td>
</tr>
<tr>
<td>configure manager delete</td>
<td>Removes the managing Firepower Management Center.</td>
</tr>
<tr>
<td>show managers</td>
<td>Shows the current manager.</td>
</tr>
</tbody>
</table>
configure network dns searchdomains

To configure the list of DNS search domains, use the `configure network dns searchdomains` command.

```
configure network dns searchdomains [dnslist]
```

**Syntax Description**
- `dnslist`: Specifies a comma-separated list of DNS search domains.

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

Use this command to replace the current list of DNS search domains with a new list. These domains are added to hostnames when you do not specify a fully-qualified domain name in a command, for example, `ping system`. The domains are used on the management interface, or for commands that go through the management interface, only.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

**Examples**

The following example configures a new search domains list and then ping’s a hostname that is not fully-qualified.

```
> configure network dns searchdomains example.com
> show dns system
search example.com
nameserver 10.163.47.11
> ping system www
PING www.example.com (10.163.4.161) 56(84) bytes of data.
64 bytes from www.example.com (10.163.4.161): icmp_seq=1 ttl=242 time=8.01 ms
64 bytes from www.example.com (10.163.4.161): icmp_seq=2 ttl=242 time=16.7 ms
^C
--- origin-www.cisco.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 7.961/10.216/16.718/3.755 ms
```
configure network dns servers

To configure the DNS servers for the management interface, use the `configure network dns servers` command.

```
configure network dns servers [dnslist]
```

**Syntax Description**

- `dnslist` Specifies a comma-separated list of DNS servers.

**Command History**

```
Release Modification
6.1 This command was introduced.
```

**Usage Guidelines**

Use this command to replace the current list of DNS servers with a new list. The servers are used on the management interface only. They cannot resolve fully-qualified domain names for commands that go through the data interfaces.

Starting with version 6.3, for locally-managed devices only, if the data and management interfaces are using the same DNS group, the group is updated on your next deployment from the manager, which means that the changes are also applied to the DNS group used on the data interfaces. The changes for the management interface are immediate. We recommend that you make all DNS changes from the local manager rather than use this command.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

**Examples**

The following example configures the DNS servers for the management interface.

```
> configure network dns servers 10.163.47.11,10.124.1.10
> show dns system
search example.com
nameserver 10.163.47.11
nameserver 10.124.1.10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure network dns</code></td>
<td>Configures DNS search domains.</td>
</tr>
<tr>
<td><code>searchdomains</code></td>
<td>Shows the current DNS configuration for the management interface.</td>
</tr>
</tbody>
</table>
configure network hostname

To configure the hostname for the device’s management interface, use the `configure network hostname` command.

```
configure network hostname  name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the new hostname.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The system hostname is defined in more than one place. If you update the hostname from the manager, the system synchronizes the hostname across all processes. If you use this command when using Firepower Device Manager (the local manager), you need to deploy changes from Firepower Device Manager to complete the update so that the same name is used by all system processes.

**Examples**

The following example sets the hostname to sfrocks.

```
> configure network hostname sfrocks
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show network</td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network http-proxy

To configure an HTTP proxy for the management interface, use the `configure network http-proxy` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to set up an HTTP Proxy address for the device. After issuing the command, you are prompted for the HTTP proxy address and port, whether proxy authentication is required, and if it is required, the proxy username, proxy password, and confirmation of the proxy password.

**Note**

The HTTP proxy is supported for use with the remote manager only. It is not supported when using the local manager, Firepower Device Manager.

**Examples**

The following example configures an HTTP proxy for the management interface. In this example, authentication is configured. The CLI does not display the password that you type.

```plaintext
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure network http-proxy-disable</td>
<td>Disables HTTP Proxy settings.</td>
</tr>
<tr>
<td>show network</td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network http-proxy-disable

To remove the HTTP proxy for the management interface, use the `configure network http-proxy-disable` command.

**configure network http-proxy-disable**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example removes the HTTP proxy for the management interface.

```plaintext
> show network
(...) Output Truncated...
-------------------[ Proxy Information ]-------------------
State : Enabled
HTTP Proxy : 10.100.10.10
Port : 80
Authentication : Enabled
Username : proxyuser
```

> `configure network http-proxy-disable`

Are you sure that you wish to delete the current http-proxy configuration? (y/n): y

Configuration successfully deleted.

> show network

(...) Output Truncated...
-------------------[ Proxy Information ]-------------------
State : Disabled
Authentication : Disabled
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure network http-proxy</code></td>
<td>Configures HTTP Proxy settings.</td>
</tr>
<tr>
<td><code>show network</code></td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
**configure network ipv4 delete**

To disable the IPv4 configuration of the device’s management interface, use the `configure network ipv4 delete` command.

```
configure network ipv4 delete  [management_interface]
```

**Syntax Description**

- `management_interface`: Specifies the management interface. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the `configure management-interface` commands to enable more than one management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. Do not specify this parameter for other platforms. The management interface IDs on the Firepower 4100 and 9300 are `management0` for the default management interface and `management1` for the optional event interface.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to disable the IPv4 configuration of the device’s management interface. If you are connected to the IP address you delete, you will lose your connection to the device. Ensure that you have an IPv6 address configured before removing the IPv4 address.

You do not need to delete the configuration to change the IPv4 address. Use the `configure network ipv4 manual` or `configure network ipv4 dhcp` commands if you want to keep IPv4 addressing but you simply want to change the address.

**Examples**

The following example deletes the IPv4 address configuration.

```
> configure network ipv4 delete
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure network ipv4 dhcp</td>
<td>Configures IPv4 to obtain an address from a DHCP server.</td>
</tr>
<tr>
<td>configure network ipv4 manual</td>
<td>Configures IPv4 manually with a static IP address.</td>
</tr>
<tr>
<td>show network</td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network ipv4 dhcp

To configure the management interface to obtain an IPv4 address from a DHCP server, use the configure network ipv4 dhcp command.

```plaintext
configure network ipv4 dhcp
```

### Syntax Description

- **management_interface**
  - Specifies the management interface. DHCP is supported only on the default management interface, so you do not need to use this argument.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to specify that the device’s management interface receives its IPv4 configuration from a DHCP server. The management interface communicates with the DHCP server to obtain its configuration information.

### Examples

The following example configures the management interface to obtain its IPv4 address using DHCP.

```plaintext
> configure network ipv4 dhcp
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure network ipv4</td>
<td>Disables IPv4 networking.</td>
</tr>
<tr>
<td>delete</td>
<td></td>
</tr>
<tr>
<td>configure network ipv4</td>
<td>Configures IPv4 manually.</td>
</tr>
<tr>
<td>manual</td>
<td></td>
</tr>
<tr>
<td>show network</td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network ipv4 dhcp-server-disable

To disable the DHCP server on the management interface, use the `configure network ipv4 dhcp-server-disable` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If there is an active DHCP server on the management interface, you can disable it. When disabled, clients on the management network will either have to configure static addresses, or you will need to configure a different device on the network to provide DHCP server services.

If you change the management IP address to use DHCP to obtain an address, the DHCP server (if enabled) is automatically disabled.

**Examples**

The following example shows how to check whether DHCP server is enabled, and then how to disable it.

```
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
> configure network ipv4 dhcp-server-disable
DHCP Server Disabled
> show network-dhcp-server
DHCP Server Disabled
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure network ipv4 dhcp-server-enable</code></td>
<td>Enables the DHCP server on the management interface.</td>
</tr>
<tr>
<td><code>show dhcp-server</code></td>
<td>Shows the status of the DHCP server on the management interface.</td>
</tr>
</tbody>
</table>
**configure network ipv4 dhcp-server-enable**

To enable the optional DHCP server on the management interface, use the `configure network ipv4 dhcp-server-enable` command.

```
configure network ipv4 dhcp-server-enable  start_ip_address  end_ip_address
```

**Syntax Description**

- `start_ip_address`: Specifies the starting and ending IPv4 addresses for the DHCP address pool. When the management interface receives a DHCP client request, it provides an address from this pool. The pool must be on the same subnet as the management IPv4 address.
- `end_ip_address`: Do not include the network address, management address, or broadcast address in the DHCP address pool.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you configure a manual (static) IPv4 address for the management interface, you can configure a DHCP server to supply addresses to endpoints on the management network.

Before enabling the server, ensure that there is no other DHCP server on the management network. You can have at most one DHCP server per network, or results can be unpredictable.

**Note**

This command is not supported on Firepower Threat Defense Virtual devices.

**Examples**

The following example shows how to configure the DHCP server and show its status.

```
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure network ipv4</td>
<td>Disables the DHCP server on the management interface.</td>
</tr>
<tr>
<td>dhcp-server-disable</td>
<td></td>
</tr>
<tr>
<td>show dhcp-server</td>
<td>Shows the status of the DHCP server on the management interface.</td>
</tr>
</tbody>
</table>
configure network ipv4 manual

To configure a static IPv4 address on the management interface, use the `configure network ipv4 manual` command.

`configure network ipv4 manual  ipaddr  netmask  gw  [management_interface]`

**Syntax Description**

- **ipaddr**: Specifies the IP address.
- **netmask**: Specifies the subnet mask.
- **gw**: Specifies the IPv4 address of the default gateway.

If you are using the local manager, Firepower Device Manager, you have the option of specifying `data-interfaces`, which uses the data interfaces on the device as a gateway instead of an explicit gateway on the management network. Use the data interfaces if you do not want to wire the management physical interface to a separate management network.

The `data-interfaces` keyword is not supported for Firepower Threat Defense Virtual.

Note that the `gw` in this command is only used to create the default route for the primary management interface. If you set the gateway for an event-only interface, then this command ignores the gateway and does not create a default or static route for it. You must create a static route separately using the `configure network static-routes` command.

- **management_interface**: Specifies the management interface. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the `configure management-interface` commands to enable more than one management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. Do not specify this parameter for other platforms. The management interface IDs on the Firepower 4100 and 9300 are `management0` for the default management interface and `management1` for the optional event interface.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2</td>
<td>The <code>data-interfaces</code> keyword was added for gateway.</td>
</tr>
</tbody>
</table>

**Examples**

The following example configures a static IPv4 address on the management interface.

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure network ipv4</code></td>
<td>Enables IPv4 networking.</td>
</tr>
<tr>
<td><code>delete</code></td>
<td></td>
</tr>
<tr>
<td><code>configure network ipv4</code></td>
<td>Configures IPv4 via DHCP.</td>
</tr>
<tr>
<td><code>dhcp</code></td>
<td></td>
</tr>
<tr>
<td><code>show network</code></td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network ipv6 delete

To disable the IPv6 configuration of the device’s management interface, use the `configure network ipv4 delete` command.

`configure network ipv6 delete  [management_interface]`

**Syntax Description**

| management_interface | Specifies the management interface. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the `configure management-interface` commands to enable more than one management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. Do not specify this parameter for other platforms. The management interface IDs on the Firepower 4100 and 9300 are management0 for the default management interface and management1 for the optional event interface. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to disable the IPv6 configuration of the device’s management interface. If you are connected to the IP address you delete, you will lose your connection to the device. Ensure that you have an IPv4 address configured before removing the IPv6 address.

You do not need to delete the configuration to change the IPv6 address. Use the `configure network ipv6 {manual | dhcp | router}` commands if you want to keep IPv6 addressing but you simply want to change the address.

**Examples**

The following example deletes the IPv6 address configuration.

```
> configure network ipv6 delete
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure network ipv6 dhcp</td>
<td>Configures IPv6 via DHCP.</td>
</tr>
<tr>
<td>configure network ipv6 manual</td>
<td>Configure IPv6 manually.</td>
</tr>
<tr>
<td>configure network ipv6 router</td>
<td>Configure IPv6 via router.</td>
</tr>
<tr>
<td>show network</td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network ipv6 destination-unreachable

To enable or disable ICMPv6 Destination Unreachable packets when using IPv6 on the management interface, use the `configure network ipv6 destination-unreachable` command.

```shell
configure network ipv6 destination-unreachable { enable | disable }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables Destination Unreachable packets. This setting is the default.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables Destination Unreachable packets.</td>
</tr>
</tbody>
</table>

**Command Default**

Enabled by default.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.0</td>
<td>Command added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You might want to disable these packets to guard against potential denial of service attacks.

**Examples**

The following example disables the Destination Unreachable message.

```shell
> configure network ipv6 destination-unreachable disable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure network ipv6 delete</code></td>
<td>Disables IPv6 networking.</td>
</tr>
<tr>
<td><code>configure network ipv6 echo-reply</code></td>
<td>Enables or disables Echo Reply packets.</td>
</tr>
<tr>
<td><code>configure network ipv6 manual</code></td>
<td>Configures IPv6 manually.</td>
</tr>
<tr>
<td><code>configure network ipv6 router</code></td>
<td>Configures IPv6 via router.</td>
</tr>
<tr>
<td><code>show network</code></td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network ipv6 dhcp

To configure the management interface to obtain an IPv6 address from a DHCP server, use the `configure network ipv6 dhcp` command.

`configure network ipv6 dhcp [management_interface]`

**Syntax Description**

- `management_interface`: Specifies the management interface. DHCP is supported only on the default management interface, so you do not need to use this argument.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to specify that the device’s management interface receives its IPv6 configuration from a DHCP server. The management interface communicates with the DHCP server to obtain its configuration information.

**Examples**

The following example configures the management interface to obtain its IPv6 address using DHCP.

```
> configure network ipv6 dhcp
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure network ipv6 delete</code></td>
<td>Disables IPv6 networking.</td>
</tr>
<tr>
<td><code>configure network ipv6 manual</code></td>
<td>Configure IPv6 manually.</td>
</tr>
<tr>
<td><code>configure network ipv6 router</code></td>
<td>Configure IPv6 via router.</td>
</tr>
<tr>
<td><code>show network</code></td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network ipv6 echo-reply

To enable or disable ICMPv6 Echo Reply packets when using IPv6 on the management interface, use the `configure network ipv6 echo-reply` command.

```
configure network ipv6 echo-reply {enable | disable}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables Echo Reply packets. This setting is the default.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables Echo Reply packets.</td>
</tr>
</tbody>
</table>

**Command Default**

Enabled by default.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.0</td>
<td>Command added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You might want to disable these packets to guard against potential denial of service attacks. Disabling Echo Reply packets means you cannot use IPv6 ping to the device management interfaces for testing purposes.

**Examples**

The following example disables the Echo Reply message.

```
> configure network ipv6 echo-reply disable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure network ipv6 delete</td>
<td>Disables IPv6 networking.</td>
</tr>
<tr>
<td>configure network ipv6 destination-unreachable</td>
<td>Enables or disables Destination Unreachable packets.</td>
</tr>
<tr>
<td>configure network ipv6 manual</td>
<td>Configures IPv6 manually.</td>
</tr>
<tr>
<td>configure network ipv6 router</td>
<td>Configures IPv6 via router.</td>
</tr>
<tr>
<td>show network</td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network ipv6 manual

To configure a static IPv6 address on the management interface, use the `configure network ipv6 manual` command.

`configure network ipv6 manual ip6addr ip6prefix [ip6gw] [management_interface]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip6addr</td>
<td>Specifies the IP address.</td>
</tr>
<tr>
<td>ip6prefix</td>
<td>Specifies the prefix length.</td>
</tr>
<tr>
<td>ip6gw</td>
<td>Specifies the IPv6 address of the default gateway.</td>
</tr>
</tbody>
</table>

- If you are using the local manager, Firepower Device Manager, you have the option of specifying `data-interfaces`, which uses the data interfaces on the device as a gateway instead of an explicit gateway on the management network. Use the data interfaces if you do not want to wire the management physical interface to a separate management network.

  The `data-interfaces` keyword is not supported for Firepower Threat Defense Virtual.

- Note that the `ip6gw` in this command is only used to create the default route for the primary management interface. If you set the gateway for an event-only interface, then this command ignores the gateway and does not create a default or static route for it. You must create a static route separately using the `configure network static-routes` command.

- `management_interface` Specifies the management interface. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the `configure management-interface` commands to enable more than one management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. Do not specify this parameter for other platforms. The management interface IDs on the Firepower 4100 and 9300 are `management0` for the default management interface and `management1` for the optional event interface.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2</td>
<td>The <code>data-interfaces</code> keyword was added for gateway.</td>
</tr>
</tbody>
</table>

**Examples**

The following example configures a static IPv6 address for the management interface.

```
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure network ipv6 delete</code></td>
<td>Disables IPv6 networking.</td>
</tr>
<tr>
<td><code>configure network ipv6 dhcp</code></td>
<td>Configures IPv6 via DHCP.</td>
</tr>
<tr>
<td><code>configure network ipv6 router</code></td>
<td>Configure IPv6 via router.</td>
</tr>
<tr>
<td><code>show network</code></td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network ipv6 router

To configure the management interface to obtain an IPv6 address from a router using stateless autoconfiguration, use the `configure network ipv6 router` command.

```
configure network ipv6 router [management_interface]
```

**Syntax Description**

- `management_interface`: Specifies the management interface. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the `configure management-interface` commands to enable more than one management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. Do not specify this parameter for other platforms. The management interface IDs on the Firepower 4100 and 9300 are `management0` for the default management interface and `management1` for the optional event interface.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to specify that the device’s management interface receives its IPv6 configuration from a router. The management interface communicates with the IPv6 router to obtain its configuration information.

**Examples**

The following example configures the management interface to receive its IPv6 address from a router using stateless autoconfiguration.

```
> configure network ipv6 router
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure network ipv6 delete</code></td>
<td>Disables IPv6 networking.</td>
</tr>
<tr>
<td><code>configure network ipv6 dhcp</code></td>
<td>Configures IPv6 via DHCP.</td>
</tr>
<tr>
<td><code>configure network ipv6 manual</code></td>
<td>Configure IPv6 manually.</td>
</tr>
<tr>
<td><code>show network</code></td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network management-interface

To configure multiple management interfaces to separate event and management traffic on Firepower 4100 or 9300 series devices, use the configure network management-interface command. For Firepower Threat Defense, multiple management interfaces are available for Firepower 4100 and 9300 series devices only. You can also use this command to set the TCP port used for FMC communication.

```
configure network management-interface { [ disable | disable-event-channel | disable-management-channel ] interface_id } | tcpport number }
```

### Syntax Description

- **disable**
  - Disables the specified management interface.

- **disable-event-channel**
  - Disables the event channel on the specified interface.

- **disable-management-channel**
  - Disables the management channel on the specified interface.

- **enable**
  - Enables the specified management interface.

- **enable-event-channel**
  - Enables the event channel on the specified interface.

- **enable-management-channel**
  - Enables the management channel on the specified interface.

- **interface_id**
  - Specifies the management interface that you want to enable or disable, management0 or management1. management0 and management1 are the internal names of these interfaces, regardless of the physical interface ID.

- **tcpport number**
  - Configures the TCP port used for communications with the Firepower Management Center. The default is 8305. Do not specify the SSH (22) or HTTPS (443) ports if you change the default. Keep the number in the high range above 1024, up to 65535. This command is equivalent to the configure network management-port command.

### Command Default

The management0 interface is enabled, and used for both event and management traffic. management1 is disabled.

The default TCP port is 8305.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

For device management, the Firepower Management Center management interface carries two separate traffic channels: the management traffic channel carries all internal traffic (such as inter-device traffic specific to the management of the device), and the event traffic channel carries all event traffic (such as web events). You can optionally configure a separate event-only interface on the FMC to handle event traffic (see the FMC web interface do perform this configuration). You can only configure one event-only interface. Event traffic can use a large amount of bandwidth, so separating event traffic from management traffic can improve the performance of the Management Center.
On Firepower 4100 and 9300 series devices, the mgmt-type interface that you assign to the logical device is designated as the default management0 interface in the Firepower Threat Defense application. This interface includes both management and event channels by default. If you configured a separate event interface on the FMC, then on the Firepower 4100 or 9300 device, you can optionally assign a firepower-eventing-type interface to the Firepower Threat Defense logical device to take advantage of the separation. This interface is designated as the management1 interface. Event traffic is sent between the device event interface and the FMC event interface if possible. If the event network goes down, then event traffic reverts to the default management interface. Separate event interfaces are used when possible, but the management interface is always the backup.

The FMC event-only interface cannot accept management channel traffic, so you should simply disable the management channel on the device event interface. You can optionally disable events for the management interface. In either case, the device will try to send events on the event-only interface, and if that interface is down, it will send events on the management interface even if you disable the event channel.

After you assign the event interface to the logical device, this interface is not enabled or configured with network settings. You must access the Firepower Threat Defense CLI and use the `configure network management-interface` command to enable it. Then use the `configure network {ipv4 | ipv6} manual` commands to configure the address(es) for this interface.

**Examples**

The following example enables management1, and disables the management channel. By default, both channels are enabled.

```
> configure network management-interface enable management1
> configure network management-interface disable-management-channel management1
>
```

The following example changes the port used for communications with the Firepower Management Center.

```
> configure network management-interface tcpport 8306
Management port changed to 8306.
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure network static-routes ipv4/ipv6</td>
<td>Configures static routes for the management interface.</td>
<td></td>
</tr>
<tr>
<td>show network</td>
<td>Shows the management interface configuration.</td>
<td></td>
</tr>
</tbody>
</table>
configure network management-port

To configure the TCP port used for communicating with Firepower Management Center, use the `configure network management-port` command.

```
configure network management-port  number
```

**Syntax Description**

<table>
<thead>
<tr>
<th><code>number</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the TCP port used for communications with the Firepower Management Center. The default is 8305. Do not specify the SSH (22) or HTTPS (443) ports if you change the default. Keep the number in the high range above 1024, up to 65535.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to change the port used for management connections to the Firepower Management Center. This command does not change the port used for the local manager, Firepower Device Manager. This command is equivalent to the `configure network management-interface tcpport` command; you do not need to use both commands.

**Examples**

The following example changes the port used for communications with the Firepower Management Center.

```
> configure network management-port 8306
Management port changed to 8306.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure network ipv4</code></td>
<td>Configures IPv4 addressing for the management interface.</td>
</tr>
<tr>
<td><code>configure network ipv6</code></td>
<td>Configures IPv6 addressing for the management interface.</td>
</tr>
<tr>
<td><code>show network</code></td>
<td>Shows the management interface configuration.</td>
</tr>
</tbody>
</table>
configure network static-routes

To add or remove static routes when using multiple management interfaces, use the configure network static-routes command. Multiple interfaces are supported on Firepower 4100 and 9300 series devices only.

configure network static-routes {ipv4 | ipv6} {add interface destination netmask_or_prefix gateway | delete}

Syntax Description

| add | Adds a static route for the management interface. |
| delete | Removes a static route for the management interface. You are prompted to choose which route to delete. |
| interface | The ID of the management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. The management interface IDs on the Firepower 4100 and 9300 are management0 for the main management interface and management1 for the optional event interface. |
| ipv4 | Adds or deletes a static route for the IPv4 management address. |
| ipv6 | Adds or deletes a static route for the IPv6 management address. |
| destination | The destination IP address to add or remove, in IPv4 or IPv6 format as appropriate. For example, 10.100.10.10 or 2001:db8::201. |
| netmask_or_prefix | The network address mask for IPv4, or prefix for IPv6. The IPv4 netmask must be in dotted decimal format, for example, 255.255.255.0. The IPv6 prefix is a standard prefix number, such as 96. |
| gateway | The gateway address to add or remove, in IPv4 or IPv6 format as appropriate. |

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you configure an event-only interface using the configure network management-interface commands, you need to configure a static route if this interface is on a separate network from the management interface. Static routes do not affect through-the-box traffic, i.e. traffic on data interfaces. Without static routes, all management traffic uses the default route specified as the gateway for the default management interface. You typically do not need static routes when using a single management interface, or if the event-only interface is on the same network.

For the default route, do not use this command; you can only change the default route gateway IP address when you use the configure network ipv4 or ipv6 commands for the default management interface.
Examples

The following example adds an IPv4 static route for management interface management1, using a destination address of 10.115.24.0, a network address mask of 255.255.255.0, and a gateway address of 10.115.9.2:

```
> configure network static-routes ipv4 add management1 10.115.24.0 255.255.255.0 10.115.9.2
```

The following example adds an IPv6 static route for management interface management1, using a destination address of 2001:db8::201, an IPv6 prefix length of 64, and a gateway address of 2001:db8::3657:

```
> configure network static-routes ipv6 add management1 2001:db8::201 64 2001:db8::3657
```

The following example shows how to delete a static route.

```
> show network-static-routes
---------------------[ IPv4 Static Routes ]---------------------
Interface           : management1
Destination          : 10.1.1.0
Gateway              : 192.168.0.254
Netmask              : 255.255.255.0
> configure network static-routes ipv4 delete
Please select which IPv4 Static Route to delete:
1) management1: dest 10.1.1.0 nmask 255.255.255.0 gw 192.168.0.254
Please enter number of route to delete: 1
Interface: management1
Destination: 10.1.1.0
Netmask: 255.255.255.0
Gateway: 192.168.0.254
Are you sure that you want to delete this route? (y/n) [n]: y
Configuration updated successfully
> show network-static-routes
No static routes currently configured.
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure network management-interface</td>
<td>Configures multiple management interfaces.</td>
</tr>
<tr>
<td>configure network static-routes ipv4</td>
<td>Adds or removes an IPv4 static route for the management interface.</td>
</tr>
<tr>
<td>show network-static-routes</td>
<td>Shows static routes configured for the management interfaces.</td>
</tr>
</tbody>
</table>
configure password

To change the password for the user account you are currently logged into, use the `configure password` command.

```
configure password
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Using this command, the current user can change their password in CLI. After issuing the command, the CLI prompts the user for their current (or old) password, then prompts the user to enter the new password twice.

**Examples**

The following example changes the password for the current user account.

```
> configure password
Enter current password: oldpassword
Enter new password: newpassword
Confirm new password: newpassword
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure user add</td>
<td>Adds a user account for CLI access.</td>
</tr>
</tbody>
</table>
configure snort

To configure advanced behavior for the Snort inspection engine, use the `configure snort` command.

```plaintext
configure snort  preserve-connection  { enable  |  disable }
```

### Syntax Description

- **preserve-connection**
  - `{ enable  |  disable }

Whether to preserve existing TCP/UDP connections on routed and transparent interfaces in case the Snort process goes down. This option is enabled by default, but you can disable it. When enabled, connections that were already allowed remain established, but new connections cannot be established until Snort is again available. When disabled, all new or existing connections are dropped when Snort goes down.

Non-TCP/UDP connections, such as ICMP pings, are not preserved.

To view the current setting, use the `show running-config snort` command. When viewing the entire running configuration, the `no` form of the `snort preserve-connection` command indicates the feature is disabled.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.0.2, 6.2.3</td>
<td>This command was introduced. However, <code>preserve-connection disable</code> is not supported with Firepower Device Manager (local management), which re-enables preserve-connection every time it deploys the configuration. This command is not available when the Firepower Threat Defense or Firepower Management Center is running Version 6.2.1, 6.2.2, 6.2.2.x, or a version earlier than 6.2.0.2, in which case the device behaves as if the command is disabled, whereby all new or existing connections are dropped when Snort goes down.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

With `preserve-connection` enabled, if Snort goes down, any existing connections remain established. When Snort becomes available, these established connections continue to bypass Snort inspection. Any new connections that require Snort inspection are dropped until Snort becomes available again.

### Example

The following example disables `preserve-connection`.

```plaintext
> configure snort  preserve-connection  disable
```

### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show conn</code></td>
<td>Shows connections.</td>
</tr>
<tr>
<td><code>show conn detail</code></td>
<td>Includes snort inspection information in connection details.</td>
</tr>
<tr>
<td><code>show conn detail long</code></td>
<td>Includes snort inspection information in long-format connection details.</td>
</tr>
</tbody>
</table>
**configure ssh-access-list**

To configure the device to accept SSH connections from specified IP addresses, use the **configure ssh-access-list** command.

```plaintext
configure ssh-access-list address_list
```

**Syntax Description**

- **address_list**: A comma separated list of IP addresses for hosts or networks, in IPv4 Classless Inter-Domain Routing (CIDR) notation or IPv6 prefix length notation. For example, 10.100.10.0/24 or 2001:DB8::/96.

  To specify all IPv4 hosts, enter 0.0.0.0/0. To specify all IPv6 hosts, specify ::/0.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must include all supported hosts or networks in a single command. Addresses specified in this command overwrite the current contents of the SSH access list.

Merely allowing SSH access does not permit users to log into the local manager. Access to the configuration software is controlled by username and password.

If you exclude the IP address from which you are currently logged into the CLI, your connect will be broken. You will need to change your IP address to regain entry into the CLI.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

**Examples**

The following example configures the device to accept SSH connections from any IPv4 or IPv6 address:

```plaintext
> configure ssh-access-list 0.0.0.0/0,::/0
The ssh access list was changed successfully.
> show ssh-access-list
  ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh
  ACCEPT tcp anywhere anywhere state NEW tcp dpt:ssh
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>Clears the SSH access list.</td>
</tr>
<tr>
<td>disable-ssh-access</td>
<td></td>
</tr>
<tr>
<td>show ssh-access-list</td>
<td>Shows the SSH access list.</td>
</tr>
</tbody>
</table>
configure ssl-protocol

To configure the SSL protocols clients can use in HTTPS connections to the device, when using the local manager, use the `configure ssl-protocol` command.

```
configure ssl-protocol  (protocol_list | default)
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Enables the default SSL protocol list: TLSv1.1, TLSv1.2.</td>
</tr>
<tr>
<td>protocol_list</td>
<td>A comma-separated list specifying any of the following protocols: TLSv1, TLSv1.1, TLSv1.2, SSLv3.</td>
</tr>
</tbody>
</table>

**Command Default**

The default setting is TLSv1.1, TLSv1.2.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command sets the protocols clients can use for HTTPS web access to the device. This is used with the local manager, Firepower Device Manager. It is not used with a remote manager.

**Note**

If you use this command to disable the protocol you are currently using to communicate with the device, you will lose the connection.

**Examples**

The following example configures the device to accept all SSL protocols for HTTPS connections.

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
> configure ssl-protocol TLSv1,TLSv1.1,TLSv1.2,SSLv3
The following ssl protocols are now enabled: TLSv1 TLSv1.1 TLSv1.2 SSLv3
> show ssl-protocol
The supported ssl protocols are TLSv1 TLSv1.1 TLSv1.2 SSLv3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ssl-protocol</td>
<td>Shows the currently configured SSL protocols.</td>
</tr>
</tbody>
</table>
configure tcp-randomization

To disable TCP sequence number randomization, use the `configure tcp-randomization` command.

```
configure tcp-randomization {enable | disable}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Change TCP sequence numbers in incoming and outgoing packets randomly to prevent attackers from anticipating the next packet's sequence number.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Do not change TCP sequence numbers in incoming and outgoing packets.</td>
</tr>
</tbody>
</table>

**Command Default**
TCP sequence number randomization is enabled by default.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Each TCP connection has two initial sequence numbers (ISNs): one generated by the client and one generated by the server. The Firepower Threat Defense device randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predicting the next ISN for a new connection and potentially hijacking the new session.

You can disable TCP initial sequence number randomization if necessary, for example, because data is getting scrambled. For example, you might be using a software test tool, software product, or hardware device that depends on TCP packets having sequential numbering. Changing the TCP randomization setting affects all interfaces and all traffic on the device; you cannot change it for specific interfaces or traffic classes.

You should disable TCP sequence number randomization only if you encounter specific problems due to randomization.

**Note**

Although you can disable TCP sequence number randomization when using Firepower Device Manager, each time you deploy the configuration from Firepower Device Manager, the feature is re-enabled. If you want to keep TCP sequence number randomization disabled, you must re-enter the command after each deployment.

**Example**

The following example disables TCP sequence number randomization.

```
> configure tcp-randomization disable
```

To determine if TCP sequence number randomization is currently enabled or disabled, look in the running configuration for the `set connection random-sequence-number disable` command. This command will be in the global_policy policy map, so you can limit your view of the configuration by using the `show running-config policy-map` command. If the `set connection`
**random-sequence-number** command does not appear in the configuration, then TCP sequence number randomization is enabled.

For example, the following shows that TCP sequence number randomization is disabled (the relevant command is highlighted).

```plaintext
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
    inspect ip-options
    inspect icmp
    inspect icmp error
  class tcp
    set connection random-sequence-number disable
!
```

The following example shows that TCP sequence number randomization is enabled because the **set connection random-sequence-number** command is not in the global_policy policy map.

```plaintext
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
    inspect ip-options
```
inspect icmp
inspect icmp error
**configure unlock_time**

To set the length of time after which a user account is automatically unlocked after being locked for exceeding the maximum number of failed logins, use the `configure unlock_time` command. This command works in CC/UCAPL compliance mode only.

```
configure unlock_time  number
```

**Syntax Description**

| `number` | Specifies the unlock time in minutes, from 1 to 9999. |

**Command Default**

When running in CC/UCAPL mode, the default unlock time is 30 minutes.

When not running in CC/UCAPL mode, user accounts remain locked until you unlock them using the `configure user unlock` command. You cannot set an automatic unlock time.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you are running in CC/UCAPL compliance mode, you can set a global unlock time for locked out users. After the time expires for a given user who has exceeded the maximum failed login attempts for the user account, the account is unlocked and the user can try again. Use the `configure user maxfailedlogins` command to set the maximum number of failed login attempts you will allow.

Even with an unlock time set, you can unlock a user account at any time using the `configure user unlock` command. The user does not need to wait for the unlock time to expire.

**Example**

The following example configures an unlock time of 60 minutes.

```
> configure unlock_time 60
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure user add</td>
<td>Adds a new user.</td>
</tr>
<tr>
<td>configure user maxfailedlogins</td>
<td>Sets the maximum number of failed logins allowed for a user.</td>
</tr>
<tr>
<td>configure user unlock</td>
<td>Unlocks the account for the specified user.</td>
</tr>
<tr>
<td>show user</td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
configure user access

To change the access authorization level for an existing user, use the `configure user access` command.

```
configure user access  username  {basic  |  config}
```

**Syntax Description**

- `username` Specifies the name of the existing user.
- `basic` Gives the user basic access. This does not allow the user to enter configuration commands.
- `config` Gives the user configuration access. This gives the user full administrator rights to all commands.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you create a user account, you specify the user’s access rights. Use the `configure user access` command to modify the access level of the specified user. The command takes effect the next time the user logs in.

**Examples**

The following example changes user jdoe’s access rights to Basic.

```
> configure user access jdoe basic
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure user add</td>
<td>Adds a new user.</td>
</tr>
<tr>
<td>show user</td>
<td>Shows the user accounts and access rights.</td>
</tr>
</tbody>
</table>
configure user add

To create a new user account for CLI access, use the `configure user add` command.

```
configure user add  username  (basic  |  config)
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Specifies the name of the existing user.</td>
<td></td>
</tr>
<tr>
<td>basic</td>
<td>Gives the user basic access. This does not allow the user to enter configuration commands.</td>
<td></td>
</tr>
<tr>
<td>config</td>
<td>Gives the user configuration access. This gives the user full administrator rights to all commands.</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to create a new user with a specified name, access level, and password. The command prompts for the password. All other account properties are configured with default properties.

Examples

The following example adds a user account named joecool with config access rights. The password is not shown as you type it.

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword

> show user
```

<table>
<thead>
<tr>
<th>Login</th>
<th>UID</th>
<th>Auth</th>
<th>Access</th>
<th>Enabled</th>
<th>Reset</th>
<th>Exp</th>
<th>Warn</th>
<th>Str</th>
<th>Lock</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>1000</td>
<td>Local</td>
<td>Config</td>
<td>Enabled</td>
<td>No</td>
<td>Never</td>
<td>N/A</td>
<td>Dis</td>
<td>No N/A</td>
<td>Dis</td>
</tr>
<tr>
<td>joecool</td>
<td>1001</td>
<td>Local</td>
<td>Config</td>
<td>Enabled</td>
<td>No</td>
<td>Never</td>
<td>N/A</td>
<td>Dis</td>
<td>No</td>
<td>5</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure user access</td>
<td>Sets user access level.</td>
</tr>
<tr>
<td>configure user aging</td>
<td>Sets user password aging.</td>
</tr>
<tr>
<td>configure user delete</td>
<td>Deletes specified user.</td>
</tr>
<tr>
<td>configure user disable</td>
<td>Disables specified user.</td>
</tr>
<tr>
<td>configure user enable</td>
<td>Enables specified user.</td>
</tr>
<tr>
<td>configure user forcereset</td>
<td>Forces password reset for specified user.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>configure user maxfailedlogins</strong></td>
<td>Sets maximum failed logins for specified user.</td>
</tr>
<tr>
<td><strong>configure user password</strong></td>
<td>Sets password for specified user.</td>
</tr>
<tr>
<td><strong>configure user strengthcheck</strong></td>
<td>Sets strength check requirement on password for specified user.</td>
</tr>
<tr>
<td><strong>configure user unlock</strong></td>
<td>Unlocks account for specified user.</td>
</tr>
<tr>
<td><strong>show user</strong></td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
configure user aging

To set an expiration date for a user’s password, use the `configure user aging` command.

```
configure user aging  username max_days warn_days
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>Specifies the name of the user. You cannot change the <code>admin</code> user aging settings.</td>
</tr>
<tr>
<td><code>max_days</code></td>
<td>Specifies the maximum number of days that the password is valid. Values range from 1 to 9999.</td>
</tr>
<tr>
<td><code>warn_days</code></td>
<td>Specifies the number of days that the user is given to change the password before it expires. Values range from 1 to 9999, but must be less than the maximum days value.</td>
</tr>
</tbody>
</table>

**Command History**

```
Release  Modification
--------  ---------------
6.1       This command was introduced.
```

**Examples**

The following example sets the user’s password to expire in 100 days, and starts warning the user 30 days before password expiration. In the show user output, note the numbers in the Exp and Warn columns.

```
> configure user aging jdoe 100 30
> show user
Login  UID  Auth Access  Enabled  Reset  Exp  Warn  Str  Lock  Max
admin 1000  Local Config Enabled  No  Never  N/A  Dis  No  N/A
jdoe   1001  Local Config Enabled  No  100  30  Dis  No  5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure user add</td>
<td>Adds a new user.</td>
</tr>
<tr>
<td>configure user forcereset</td>
<td>Forces password reset for specified user.</td>
</tr>
<tr>
<td>configure user password</td>
<td>Sets password for specified user.</td>
</tr>
<tr>
<td>show user</td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
configure user delete

To delete a user account, use the **configure user delete** command.

```plaintext
configure user delete  username
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>username</strong></td>
<td>username</td>
</tr>
<tr>
<td>Specifies the name of the user. You cannot delete the <strong>admin</strong> user.</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example deletes a user account.

```
> configure user delete jdoe
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure user add</td>
<td>Adds a new user.</td>
</tr>
<tr>
<td>configure user disable</td>
<td>Disables a user account without deleting it.</td>
</tr>
<tr>
<td>show user</td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
configure user disable

To disable a user account without deleting it, use the `configure user disable` command.

```
configure user disable  username
```

**Syntax Description**

- **username**
  
  Specifies the name of the user. You cannot disable the admin user.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to disable a user account without deleting it. Disabled users cannot login. Use the `configure user enable` command to reenable a disabled user account.

**Examples**

The following example disables a user account.

```
> configure user disable jdoe
> show user
Login  UID  Auth Access  Enabled  Reset  Exp  Warn  Str  Lock  Max
admin  1000  Local Config  Enabled  No  Never  N/A  Dis  No  N/A
jdoe   1001  Local Config  Disabled  No  100  30  Dis  No  5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure user add</td>
<td>Adds a new user.</td>
</tr>
<tr>
<td>configure user delete</td>
<td>Deletes specified user.</td>
</tr>
<tr>
<td>configure user enable</td>
<td>Enables specified user.</td>
</tr>
<tr>
<td>configure user unlock</td>
<td>Unlocks account for specified user.</td>
</tr>
<tr>
<td>show user</td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
configure user enable

To enable a previously disabled user, use the `configure user enable` command.

`configure user enable  username`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>Specifies the name of the user.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to enable a user and allow login.

**Examples**

The following example enables a disabled user account. Note the change in the `show user` Enabled column.

```
> show user
Login   UID  Auth Access  Enabled  Reset  Exp Warn  Str  Lock Max
admin   1000 Local Config  Enabled  No   Never  N/A   Dis No N/A
jdoe    1001 Local Config Disabled No  100  30 Dis No 5

> configure user enable jdoe
> show user
Login   UID  Auth Access  Enabled  Reset  Exp Warn  Str  Lock Max
admin   1000 Local Config  Enabled  No   Never  N/A   Dis No N/A
jdoe    1001 Local Config  Enabled  No   100  30 Dis No 5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure user add</code></td>
<td>Adds a new user.</td>
</tr>
<tr>
<td><code>configure user disable</code></td>
<td>Disables specified user.</td>
</tr>
<tr>
<td><code>configure user forcereset</code></td>
<td>Forces password reset for specified user.</td>
</tr>
<tr>
<td><code>configure user unlock</code></td>
<td>Unlocks account for specified user.</td>
</tr>
<tr>
<td><code>show user</code></td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
configure user forcereset

To force the user to change their password the next time they log in, use the `configure user forcereset` command.

`configure user forcereset  username`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>Specifies the name of the user.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to force the user to reset their password the next time they login. When the user logs in and changes the password, strength checking is automatically enabled.

**Examples**

The following example forces the user to reset the password on the next log in.

```
> configure user forcereset jdoe
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure user password</code></td>
<td>Sets password for specified user.</td>
</tr>
<tr>
<td><code>configure user strengthcheck</code></td>
<td>Sets strength check requirement on password for specified user.</td>
</tr>
<tr>
<td><code>show user</code></td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
configure user maxfailedlogins

To set the maximum number of consecutive failed logins for a user, use the `configure user maxfailedlogins` command.

```
configure user maxfailedlogins  username  number
```

**Syntax Description**

- `username` Specifies the name of the user.
- `number` Specifies the maximum number of consecutive failed logins, from 1 to 9999.

**Command Default**

No default behaviors or values. However, when you create a new account, the default maximum number of consecutive failed logins is 5.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.2</td>
<td>When running in CC/UCAPL compliance mode, you can also configure the maximum failed login attempts for the <code>admin</code> user.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to set the maximum number of consecutive failed logins for the specified user before their account is locked. If the user account becomes locked, use the `configure user unlock` command to unlock it.

**Examples**

The following example sets the maximum number of consecutive failed logins to 3.

```
> configure user maxfailedlogins jdoe 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure user add</code></td>
<td>Adds a new user.</td>
</tr>
<tr>
<td><code>configure user password</code></td>
<td>Sets password for specified user.</td>
</tr>
<tr>
<td><code>configure user unlock</code></td>
<td>Unlocks the account for the specified user.</td>
</tr>
<tr>
<td><code>show user</code></td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
configure user minpasswdlen

To set the minimum length for the password for a user, use the `configure user minpasswdlen` command.

```
configure user minpasswdlen  username number
```

**Syntax Description**

- `username` Specifies the name of the user.
- `number` Specifies the minimum length of the password, from 1 to 127.

**Command Default**

There is no minimum password length.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.2</td>
<td>When running in CC/UCAPL compliance mode, you can also configure a minimum password length for the <code>admin</code> user.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to set the minimum length of the password for the specified user. You are prompted for the current password for the user account. If the minimum length is longer than the current password length, you are also prompted to set a new password.

**Example**

The following example sets the minimum password length to 8 characters. In this example, the current password is less than the new minimum, so you need to set a new password.

```
> configure user minpasswdlen jdoe 8
Setting minimum password length to 8
Enter current password: <enter old password>
Enter new password for user jdoe: <enter new password>
Confirm new password for user jdoe: <enter new password>

Setting Minimum password length succeeded
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure user add</td>
<td>Adds a new user.</td>
</tr>
<tr>
<td>show user</td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>

Cisco Firepower Threat Defense Command Reference
configure user password

To set the password on another user’s account, use the configure user password command.

configure user password  username

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Specifies the name of the user.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to set a specified user’s password. This command prompts for the user’s password. To change your own password, use the configure password command instead of this command.

Examples

The following example sets the password on another user’s account. The password is not shown as you type it.

```
> configure user password jdoe
Enter new password for user jdoe: newpassword
Confirm new password for user jdoe: newpassword
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure password</td>
<td>Changes the currently logged-in user’s password.</td>
</tr>
<tr>
<td>configure user add</td>
<td>Adds a new user.</td>
</tr>
<tr>
<td>configure user aging</td>
<td>Sets user password aging.</td>
</tr>
<tr>
<td>configure user forcereset</td>
<td>Forces password reset for specified user.</td>
</tr>
<tr>
<td>configure user maxfailedlogins</td>
<td>Sets maximum failed logins for specified user.</td>
</tr>
<tr>
<td>configure user strengthcheck</td>
<td>Sets strength check requirement on password for specified user.</td>
</tr>
<tr>
<td>show user</td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
configure user strengthcheck

To enable or disable the strength requirement for a user’s password, use the configure user strengthcheck command.

```
configure user strengthcheck  username  (enable | disable)
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Specifies the name of the user. You cannot change the admin user password strength settings.</td>
</tr>
<tr>
<td>enable</td>
<td>Sets the requirement for the specified user’s password.</td>
</tr>
<tr>
<td>disable</td>
<td>Removes the requirement for the specified user’s password.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to enable or disable a strength check, which requires a user to meet specific password criteria when changing their password. When a user’s password expires or if the configure user forcereset command is used, this requirement is automatically enabled the next time the user logs in.

**Examples**

The following example enables strength checking on a user account.

```
> configure user strengthcheck jdoe enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure user add</td>
<td>Adds a new user.</td>
</tr>
<tr>
<td>configure user forcereset</td>
<td>Forces password reset for specified user.</td>
</tr>
<tr>
<td>configure user maxfailedlogins</td>
<td>Sets maximum failed logins for specified user.</td>
</tr>
<tr>
<td>configure user password</td>
<td>Sets password for specified user.</td>
</tr>
<tr>
<td>configure user unlock</td>
<td>Unlocks account for specified user.</td>
</tr>
<tr>
<td>show user</td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
**configure user unlock**

To unlocks a user account that has exceeded the maximum number of failed logins, use the `configure user unlock` command.

```
configure user unlock  username
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>Specifies the name of the user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
<td><strong>Modification</strong></td>
</tr>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example unlocks a user account.

```
> configure user unlock jdoe
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>configure user add</td>
<td>Adds a new user.</td>
</tr>
<tr>
<td>configure user</td>
<td>Sets maximum failed logins for specified user.</td>
</tr>
<tr>
<td>maxfailedlogins</td>
<td></td>
</tr>
<tr>
<td>show user</td>
<td>Shows user accounts.</td>
</tr>
</tbody>
</table>
**connect fxos**

To enter the Firepower Extensible Operation System (FXOS) Service Manager CLI mode, use the `connect fxos` command.

**connect fxos**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

FXOS is the underlying software on Firepower 2100, 4100, and 9300 series devices.

**Examples**

The following example shows how to enter the FXOS CLI when you started in the Firepower Threat Defense CLI. Enter ? to see the available commands in FXOS.

```plaintext
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2015, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are owned by other third parties and used and distributed under license.

(...remaining copyrights omitted...)
kp-fpr2100-2#
```

The following example shows what happens if you originally entered the Firepower Threat Defense CLI from the FXOS CLI (using the `connect ftd` FXOS command).

```plaintext
> connect fxos
You came from FXOS Service Manager. Please enter 'exit' to go back.
```
copy

To copy a file to or from flash memory, use the copy command.

copy [/noverify] /noconfirm (/pcap capture:/ [buffer_name] | src_url | running-config | startup-config) dest_url

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/noverify</td>
<td>(Optional) Skips the signature verification when copying development key signed images.</td>
</tr>
<tr>
<td>/noconfirm</td>
<td>Copies the file without a confirmation prompt.</td>
</tr>
<tr>
<td>/pcap capture:/ [buffer_name]</td>
<td>Copies the raw packet capture dump of the capture command from the specified buffer.</td>
</tr>
<tr>
<td>running-config</td>
<td>Specifies the running configuration stored in system memory.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Specifies the startup configuration stored in flash memory. The startup configuration is a hidden file in flash memory.</td>
</tr>
</tbody>
</table>
src-url
dest-url

Specifies the source file, the file you are copying, and the destination file, the file you are creating through the copy. You cannot copy between two remote locations, so if the source file is local, the destination file can be local or remote. If the source file is remote, the destination file must be local. Use the following URL syntax for file locations:

- disk0://[[path/][filename] or flash://[[path/][filename]—Both flash and disk0 indicates the internal Flash memory. You can use either option.
- diskn://[[path/][filename]—Indicates optional external flash drive, where n specifies the drive number.
- smb://[[path/][filename]—Indicates Server Message Block, a UNIX server local file system.
- ftp://[[user[:password]@[ ]server[[:port]][/path/]
  filename[;type=xx]]—The type can be one of these keywords: ap (ASCII passive mode), an (ASCII normal mode), ip (Default—Binary passive mode), in (Binary normal mode).
- http(s)://[[user[:password]@[ ]server[[:port]][/path/][filename]
- scp://[[user[:password]@[ ]server[/path/]
  filename[;int=interface_name]]—Indicates an SCP server. The ;int=interface option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server.
- system://[[path/][filename]—Represents the system memory.
- tftp://[[user[:password]@[ ]server[[:port][/path/]
  filename[;int=interface_name]]—Indicates a TFTP server. The path name cannot contain spaces. The ;int=interface option bypasses the route lookup and always uses the specified interface to reach the TFTP server.
- cluster_trace: —Indicates the cluster_trace file system.

---

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

After you have performed a cluster-wide capture, you can simultaneously copy the same capture file from all units in the cluster to a TFTP server by entering the following command on the master unit:

```
cluster exec copy /noconfirm /pcap capture:cap_name tftp://location/path/filename.pcap
```

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as filename_A.pcap, filename_B.pcap, where A and B are cluster unit names.

---

Note

A different destination name gets generated if you add the unit name at the end of the filename.
Examples
The following example makes a copy of the install log.

> copy /noconfirm flash:/install.log flash:/install.save.log
Copy in progress...CC
INFO: No digital signature found
150498 bytes copied in 0.20 secs

The following example shows how to copy a file from the disk to a TFTP server in the system execution space:

> copy /noconfirm disk0:/install.log
tftp://10.7.0.80/install.log

The following example shows how to copy the running configuration to a TFTP server:

> copy /noconfirm running-config tftp://10.7.0.80/firepower/device1.cfg

The following example shows how to copy a development key signed image without verifying it:

> copy /noverify /noconfirm lfbff.SSA exa_lfbff.SSA
Source filename [lfbff.SSA]?
Destination filename [exa_lfbff.SSA]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>write net</td>
<td>Copies the running configuration to a TFTP server.</td>
</tr>
</tbody>
</table>
cpu hog granular-detection

To provide real-time hog detection and set the CPU hog threshold in a short period of time, use the `cpu hog granular-detection` command.

```
cpu hog granular-detection [count number] [threshold value]
```

**Syntax Description**

- `count number` Specifies the number of code execution interruptions performed. Values are from 1-10000000. The default and recommended value is 1000.
- `threshold value` Ranges from 1 to 100. If not set, the default is used, which varies among platforms.

**Command Default**

The default `count` is 1000. The default `threshold` varies among platforms.

**Command History**

```
Release   Modification
6.1       This command was introduced.
```

**Usage Guidelines**

The `cpu hog granular-detection` command interrupts the current code execution every 10 milliseconds, and the total number of interruptions is the count. The interruption checks for CPU hogging. If there is any, it is logged. This command reduces the granularity of CPU hog detection in the data path.

Each scheduler-based hog is associated with up to 5 interrupt-based hog entries; each entry could have up to 3 tracebacks. The interrupt-based hog cannot be overwritten; if there is no space, the new one is discarded. The scheduler-based hog is still reused according to the LRU policy, and its associated interrupt-based hog is cleared by then.

**Examples**

The following example shows how to trigger CPU hog detection:

```
> cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer under heavy traffic.
Please leave time for it to finish and use show process cpu-hog to check results.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show processes cpu-hog</code></td>
<td>Displays the processes that are hogging the CPU.</td>
</tr>
<tr>
<td><code>clear process cpu-hog</code></td>
<td>Clears the processes that are hogging the CPU.</td>
</tr>
</tbody>
</table>
cpu profile activate

To start CPU profiling, use the `cpu profile activate` command.

```
cpu profile activate [n_samples] [sample-process] [process_name] [trigger cpu-usage cpu%]
```

**Syntax Description**

- `n_samples`: Allocates memory for storing `n` number of samples. Valid values are from 1 to 100,000.
- `sample-process`: Samples only a specific process.
- `process_name`: Prevents the profiler from starting until the global 5-second CPU percentage is greater and stops the profiler if the CPU percentage drops below this value.
  
  If you specify a process name, it uses the process’s 5-second CPU percentage as a trigger.

**Command Default**

The `n_samples` default value is 1000.

The `cpu%` default value is 0.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The CPU profiler can help you determine which process is using more CPU. Profiling the CPU captures the address of the process that was running on the CPU when the timer interrupt fired. This profiling occurs every 10 milliseconds, regardless of the CPU load. For example, if you take 5000 samples, the profiling takes exactly 50 seconds to complete. If the amount of CPU time that the CPU profiler uses is relatively low, the samples take longer to collect. The CPU profile records are sampled in a separate buffer.

Use the `show cpu profile` command in conjunction with the `cpu profile activate` command to display information that you can collect and that the TAC can use for troubleshooting CPU issues. The `show cpu profile dump` command output is in hexadecimal format.

If the CPU profiler is waiting for a starting condition to occur, the `show cpu profile` command displays the following output:

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```
Examples

The following example activates the profiler and instructs it to store 1000 samples, the default. Next, the `show cpu profile` command shows that the profiling is in progress. After waiting some time, the next `show cpu profile` command shows that profiling has completed. Finally, we use the `show cpu profile dump` command to get the results. Copy the output and provide it to Cisco Technical Support. You might need to log your SSH session to get the full output.

```
> cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt profiling and display the incomplete results.
> show cpu profile
CPU profiling currently in progress:
  Core 0: 501 out of 1000 samples collected.
  CP: 586 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt profiling and display the incomplete results.
> show cpu profile
CPU Profiling has stopped.
  Core 0 done with 1000 samples
  CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cpu profile</code></td>
<td>Displays the CPU profiling progress.</td>
</tr>
<tr>
<td><code>show cpu profile dump</code></td>
<td>Displays incomplete or completed results for profiling.</td>
</tr>
</tbody>
</table>

---
cpu profile dump

To save the results of CPU profiling to a text file, use the **cpu profile dump** command.

**cpu profile dump**  **dest_url**

**Syntax Description**

<table>
<thead>
<tr>
<th>dest_url</th>
</tr>
</thead>
<tbody>
<tr>
<td>• disk0:[path]/filename or flash:[path]/filename—Both flash and disk0 indicates the internal Flash memory. Can use either option.</td>
</tr>
<tr>
<td>• diskn:[path]/filename—Indicates optional external flash drive, where n specifies the drive number.</td>
</tr>
<tr>
<td>• smb:[path]/filename—Indicates a UNIX server local file system. Use Server Message Block file-system protocol in LAN managers and similar network systems to package data and exchange information with other systems.</td>
</tr>
<tr>
<td>• ftp://[user][password]@[server]:port/[path]/filename[type=xx]—The type can be one of these keywords: ap (ASCII passive mode), an (ASCII normal mode), ip (Default—Binary passive mode), in (Binary normal mode).</td>
</tr>
<tr>
<td>• http[s]://[user][password]@[server]:port/[path]/filename</td>
</tr>
<tr>
<td>• scp://[user][password]@[server]/path]/filename[:int=interface_name]—The :int=interface option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server.</td>
</tr>
<tr>
<td>• tftp://[user][password]@[server]:port/[path]/filename[:int=interface_name]—The path name cannot contain spaces. The :int=interface option bypasses the route lookup and always uses the specified interface to reach the TFTP server.</td>
</tr>
<tr>
<td>• cluster:—Indicates the cluster file system.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **CPU profile dump** command writes the CPU profiler output to a specified text file in hexadecimal format.

**Examples**

The following example stores the most recent CPU profile dump to a file named cpudump.txt:

```bash
> cpu profile dump disk0:/cpudump.txt
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cpu profile dump</code></td>
<td>Displays incomplete or completed results for profiling.</td>
</tr>
</tbody>
</table>
crashinfo force

To force the device to crash, use the crashinfo force command.

Syntax Description

- **page-fault**: Forces a crash as a result of a page fault.
- **watchdog**: Forces a crash as a result of watchdogging.
- **process process_ID**: Forces a crash of the process specified by process_ID. Use the show kernel process command to see process IDs.

Command Default
The device saves the crash information file to flash memory by default.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can use the crashinfo force command to test the crash output generation. In the crash output, there is nothing that differentiates a real crash from a crash resulting from the crashinfo force page-fault or crashinfo force watchdog command (because these are real crashes). The device reloads after the crash dump is complete.

Caution
Do not use the crashinfo force command in a production environment. The crashinfo force command crashes the device and forces it to reload.

Examples

The following example forces a crash due to a page fault.

```
> crashinfo force /noconfirm page-fault
```
crashinfo test

To test the ability of the device to save crash information to a file in flash memory, use the `crashinfo test` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Entering the `crashinfo test` command does not crash the device. If a previous crash information file already exists in flash memory, that file is overwritten.

**Examples**

The following example shows the output of a crash information file test.

```
> crashinfo test
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crashinfo</td>
<td>Clears the contents of the crash information file.</td>
</tr>
<tr>
<td>crashinfo force</td>
<td>Forces the device to crash.</td>
</tr>
<tr>
<td>show crashinfo</td>
<td>Displays the contents of the crash information file.</td>
</tr>
</tbody>
</table>
crypto ca trustpool export

To export the certificates that constitute the PKI trustpool, use the `crypto ca trustpool export` command.

```
crypto ca trustpool export  filename
```

**Syntax Description**

| filename | The file in which to store the exported trustpool certificates. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command copies the entire contents of the active trustpool to the indicated filepath in pem-coded format.

**Examples**

```
> crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
>
> more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UE.......
<More>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca trustpool import</td>
<td>Imports the certificates that constitute the PKI trustpool.</td>
</tr>
<tr>
<td>crypto ca trustpool remove</td>
<td>Removes a single certificate from the PKI trustpool.</td>
</tr>
<tr>
<td>show crypto ca trustpool</td>
<td>Shows the PKI trustpool.</td>
</tr>
</tbody>
</table>
crypto ca trustpool import

To import the certificates that constitute the PKI trustpool, use the crypto ca trustpool import command.

crypto ca trustpool import [clean] url url noconfirm [signature-required]
crypto ca trustpool import [clean] default noconfirm

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>clean</th>
<th>Removes all downloaded trustpool certificates prior to import.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>default</td>
<td>Restores the device’s default trusted CA list.</td>
</tr>
<tr>
<td></td>
<td>noconfirm</td>
<td>Suppresses all interactive prompts.</td>
</tr>
<tr>
<td></td>
<td>signature-required</td>
<td>Indicates that only signed files are accepted. If the signature-required keyword is included but the signature is not present or cannot be verified, the import fails.</td>
</tr>
</tbody>
</table>

url url

Specifies the location of the trustpool file to be imported.

- **disk0:**/[path]/[filename]—Indicates the internal Flash memory.
- **diskn:**/[path]/[filename]—Indicates optional external flash drive, where \( n \) specifies the drive number.
- **smb:**/[path]/[filename]—Indicates a UNIX server local file system. Use Server Message Block file-system protocol in LAN managers and similar network systems to package data and exchange information with other systems.
- **ftp:**/[user:[password]@] server:[port]/[path]/filename;[type=x]—The type can be one of these keywords: \( \text{ap} \) (ASCII passive mode), \( \text{an} \) (ASCII normal mode), \( \text{ip} \) (Default—Binary passive mode), \( \text{in} \) (Binary normal mode).
- **http[s]:/[user:[password]@] server:[port]/[path]/filename**
- **scp:**/[user:[password]@] server/[path]/filename[:int=interface_name]—The :int=interface option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server.
- **tftp:**/[user:[password]@] server:[port] /[path]/filename[:int=interface_name]—The pathname cannot contain spaces. The :int=interface option bypasses the route lookup and always uses the specified interface to reach the TFTP server.

---

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command provides the ability to validate the signature on the file when a trustpool bundle is downloaded from cisco.com. A valid signature is not mandatory when downloading bundles from other sources or in a
format that does not support signatures. Users are informed of the signature status and are given the option to accept the bundle or not.

The possible interactive warnings are:

• Cisco bundle format with invalid signature
• Non-cisco bundle format
• Cisco bundle format with valid signature

Note

Unless you have verified the legitimacy of the file through some other means, do not install the certificates if a file signature cannot be verified.

Examples

The following example restores the default trustpool.

```plaintext
> crypto ca trustpool import clean default noconfirm
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca trustpool export</td>
<td>Exports the certificates that constitute the PKI trustpool.</td>
</tr>
<tr>
<td>crypto ca trustpool remove</td>
<td>Removes a single certificate from the PKI trustpool.</td>
</tr>
<tr>
<td>show crypto ca trustpool</td>
<td>Shows the PKI trustpool.</td>
</tr>
</tbody>
</table>
crypto ca trustpool remove

To remove a single specified certificate from the PKI trustpool, use the **crypto ca trustpool remove** command.

**crypto ca trustpool remove**  *cert_fingerprint*  [noconfirm]

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>cert_fingerprint</em></td>
<td>The certificate fingerprint in hexadecimal.</td>
</tr>
<tr>
<td>noconfirm</td>
<td>Specify this keyword to suppress all interactive prompting.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example removes a certificate.

```
> crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crypto ca trustpool</td>
<td>Removes all certificates from the trustpool.</td>
</tr>
<tr>
<td>crypto ca trustpool export</td>
<td>Exports the certificates that constitute the PKI trustpool.</td>
</tr>
<tr>
<td>crypto ca trustpool import</td>
<td>Imports the certificates that constitute the PKI trustpool.</td>
</tr>
<tr>
<td>show crypto ca trustpool</td>
<td>Shows the PKI trustpool.</td>
</tr>
</tbody>
</table>
d - r

- debug, on page 239
- debug packet start, on page 241
- debug packet stop, on page 242
- delete, on page 243
- dir, on page 244
- dns update, on page 246
- eotool commands, on page 247
- exit, on page 248
- expert, on page 249
- failover active, on page 250
- failover exec, on page 251
- failover reload-standby, on page 254
- failover reset, on page 255
- file copy, on page 256
- file delete, on page 257
- file list, on page 258
- file secure-copy, on page 259
- fsck, on page 260
- help, on page 261
- history, on page 262
- key chain, on page 263
- logging savelog, on page 265
- logout, on page 266
- memory caller-address, on page 267
- memory delayed-free-poisoner, on page 269
- memory logging, on page 272
- memory profile enable, on page 273
- memory profile text, on page 274
- memory tracking, on page 276
- more, on page 277
- nslookup, on page 279
- packet-tracer, on page 280
- perfmon, on page 283
• pigtail commands, on page 285
• ping, on page 286
• pmtool commands, on page 289
• reboot, on page 290
• redundant-interface, on page 291
• restore, on page 292
To show debugging messages for a given feature, use the `debug` command. To disable the display of debug messages, use the `no` form of this command. Use `no debug all` to turn off all debugging commands.

```
depbug feature [subfeature] [level]
no debug feature [subfeature]
```

### Syntax Description

- **feature**: Specifies the feature for which you want to enable debugging. To see available features, use the `debug ?` command for CLI help.
- **subfeature**: (Optional) Depending on the feature, you can enable debug messages for one or more subfeatures. Use `?` to see the available subfeatures.
- **level**: (Optional) Specifies the debugging level. The level might not be available for all features. Use `?` to see the available levels.

### Command Default

The default debugging level is 1.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use `debug` commands only to troubleshoot specific problems or during troubleshooting sessions with the Cisco Technical Assistance Center (TAC). Moreover, it is best to use `debug` commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased `debug` command processing overhead will affect system use.

You can view debug output in a CLI session only. Output is directly available when connected to the Console port, or when in the diagnostic CLI (enter `system support diagnostic-cli`). You can also view output from the regular Firepower Threat Defense CLI using the `show console-output` command.

### Example

The following example enables DNS debugging and performs an action that generates messages in the diagnostic CLI. The debug messages start after the “ERROR: % Invalid Hostname” message. Press enter to get to the prompt. The example then shows what these debug messages would look like in the `show console-output` display.

```
> debug dns
debug dns enabled at level 1.

> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '? for a list of available commands.

firepower# ping www.example.com
^A
ERROR: % Invalid Hostname
firepower# DNS: get global group DefaultDNS handle 1fa0b047
```
DNS: Resolve request for 'www.example.com' group DefaultDNS
DNS: No interfaces enabled
DNS: get global group DefaultDNS handle 1fa0b047
DNS: Resolve request for 'www.example.com' group DefaultDNS
DNS: No interfaces enabled

firepower# (press Ctrl+a, then d, to return to the regular CLI.)

Console connection detached.
> show console-output
... (output redacted)...
Message #75 : DNS: get global group DefaultDNS handle 1fa0b047
Message #76 : DNS: Resolve request for 'www.cisco.com' group DefaultDNS
Message #77 : DNS: No interfaces enabled
Message #78 : DNS: get global group DefaultDNS handle 1fa0b047
Message #79 : DNS: Resolve request for 'www.cisco.com' group DefaultDNS
Message #80 : DNS: No interfaces enabled

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show debug</td>
<td>Shows the currently active debug settings.</td>
</tr>
<tr>
<td>unddebug</td>
<td>Disables debugging for a feature. This command is a synonym for no debug.</td>
</tr>
</tbody>
</table>
debug packet start

To start debugging of packets and to start writing debug logs to the debug log database, use the debug packet start command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The debug packet start opens the connection to the debug log database. Debug logs are not written to the database unless this command is invoked.

**Example**

The following example shows how to start debugging packets:

```
> debug packet start
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug packet stop</td>
<td>Closes the connection to debug logs database and stops writing debug logs to the database.</td>
</tr>
</tbody>
</table>
To stop debugging of packets and to stop writing debug logs to the debug log database, use the **debug packet stop** command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **debug packet stop** closes the connection to the debug log database.

### Example

The following example shows how to stop debugging packets:

```
> debug packet stop
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>debug packet start</strong></td>
<td>Open the connection to debug logs database and start writing debug logs to the database.</td>
</tr>
</tbody>
</table>
To delete a file from flash memory, use the `delete` command.

```
delete /noconfirm [ /recursive ] [ /replicate ] [ disk0: | diskn: | flash: ] [ path/ ] filename
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/noconfirm</td>
<td>Does not prompt for confirmation.</td>
</tr>
<tr>
<td>/recursive</td>
<td>(Optional) Deletes the specified file recursively in all subdirectories.</td>
</tr>
<tr>
<td>/replicate</td>
<td>(Optional) Deletes the specified file on the standby unit.</td>
</tr>
<tr>
<td>disk0:</td>
<td>(Optional) Specifies the internal flash memory.</td>
</tr>
<tr>
<td>diskn:</td>
<td>(Optional) Indicates optional external flash drive, where n specifies the drive number. This is typically disk1:</td>
</tr>
<tr>
<td>filename</td>
<td>Specifies the name of the file to delete.</td>
</tr>
<tr>
<td>flash:</td>
<td>(Optional) Specifies the internal flash memory. This keyword is the same as disk0.</td>
</tr>
<tr>
<td>path/</td>
<td>(Optional) Specifies to the path to the file.</td>
</tr>
</tbody>
</table>

### Command Default

If you do not specify a directory, the directory is the current working directory by default.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The file is deleted from the current working directory if a path is not specified. Wildcards are supported when deleting files.

### Examples

The following example shows how to delete a file named test.cfg in the current working directory:

```
> delete /noconfirm test.cfg
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Changes the current working directory to the one specified.</td>
</tr>
<tr>
<td>dir</td>
<td>List the files in the current directory.</td>
</tr>
<tr>
<td>rmdir</td>
<td>Removes a file or directory.</td>
</tr>
</tbody>
</table>
dir

To display the directory contents, use the dir command.

dir [/all] [all-filesystems] [/recursive] [disk0: | disk0: | flash: | system:] [path] [filename]

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/all</td>
<td>(Optional) Displays all files.</td>
</tr>
<tr>
<td>/recursive</td>
<td>(Optional) Displays the directory contents recursively.</td>
</tr>
<tr>
<td>all-filesystems</td>
<td>(Optional) Displays the files of all filesystems.</td>
</tr>
<tr>
<td>disk0:</td>
<td>(Optional) Specifies the internal Flash memory, followed by a colon.</td>
</tr>
<tr>
<td>disk0:</td>
<td>(Optional) Indicates optional external flash drive, where n specifies the drive number. This is typically disk1:</td>
</tr>
<tr>
<td>flash:</td>
<td>(Optional) Displays the directory contents of the default flash partition.</td>
</tr>
<tr>
<td>path</td>
<td>(Optional) Specifies a specific path.</td>
</tr>
<tr>
<td>filename</td>
<td>(Optional) Specifies the name of a file.</td>
</tr>
<tr>
<td>system:</td>
<td>(Optional) Displays the directory contents of the file system.</td>
</tr>
</tbody>
</table>

**Command Default**

If you do not specify a directory, the directory is the current working directory by default.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display the directory contents:

```
> dir
Directory of disk0:/
1 -rw- 1519 10:03:50 Jul 14 2003 my_context.cfg
2 -rw- 1516 10:04:02 Jul 14 2003 my_context.cfg
3 -rw- 1516 10:01:34 Jul 14 2003 admin.cfg
60985344 bytes total (60973056 bytes free)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Changes the current working directory to the one specified.</td>
</tr>
<tr>
<td>pwd</td>
<td>Displays the current working directory.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>mkdir</td>
<td>Creates a directory.</td>
</tr>
<tr>
<td>rmdir</td>
<td>Removes a directory.</td>
</tr>
</tbody>
</table>
**dns update**

To start DNS lookup to resolve the designated hostnames without waiting for the expiration of the DNS poll timer, use the `dns update` command.

```
dns update [host fqdn_name] [timeout seconds number]
```

**Syntax Description**

- **host fqdn_name**: Specifies the fully qualified domain name of the host on which to run DNS updates.
- **timeout seconds number**: Specifies the timeout for the lookup operation, in seconds, from 3-30. The default is 30.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command immediately starts a DNS lookup to resolve the designated hostnames without waiting for the expiration of the DNS poll timer. When you run DNS update without specifying a hostname, all names that are used in access control rules, which is known as being activated, are resolved. When the command finishes running, the system displays [Done] at the command prompt and generates a syslog message.

**Examples**

The following example performs a DNS update for all FQDNs used in access control rules.

```
> dns update
INFO: update dns process started
> [Done]
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear dns</td>
<td>Removes FQDN network object DNS resolutions.</td>
</tr>
<tr>
<td>show dns</td>
<td>Displays FQDN network object DNS resolutions.</td>
</tr>
</tbody>
</table>
eotool commands

Only use eotool commands under the direction of the Cisco Technical Assistance Center.
To exit from the CLI, use the `exit` command.

```plaintext
exit
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

In the regular CLI, the `exit` and `logout` commands do the same thing, closing the SSH session with the device.

When you are in expert mode, `exit` leaves expert mode and returns you to the regular CLI.

When you are in the Diagnostic CLI (system support diagnostic-cli), the `exit` command also moves you from Privileged EXEC mode back to User EXEC mode.

### Examples

The following example shows how to use the `exit` command to close the SSH connection to the CLI.

```
> exit
```

The following example shows how to use the `exit` command go from Privileged EXEC mode in the Diagnostic CLI (represented by the # sign in the prompt) back to User EXEC mode. You can ignore the Logoff message, your CLI session remains active.

```
firepower# exit
Logoff
Type help or '?' for a list of available commands.
firepower>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logout</td>
<td>Logs off from the CLI session.</td>
</tr>
</tbody>
</table>
To enter expert mode, which is required for some procedures, use the `expert` command.

```
> expert
admin@firepower:~$
admin@firepower:~$ exit
logout
>
```

**Examples**

The following example shows how to enter and exit expert mode. The expert mode prompt shows the username@hostname information.

**Usage Guidelines**

Use expert mode only if a documented procedure tells you to enter it, or if the Cisco Technical Assistance Center tells you to use it.

**Caution**

You might be able to execute commands in expert mode whose results are not reflected in Firepower Device Manager. Use documented commands only in expert mode, or commands as directed by Cisco Technical Support, to avoid unintended results.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exit from expert mode.</td>
</tr>
</tbody>
</table>
failover active

To switch a standby device to the active state, use the **failover active** command. To switch an active device to standby, use the **no** form of this command.

```bash
failover active
no failover active
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the **failover active** command to initiate a failover switch from the standby unit, or use the **no failover active** command from the active unit to initiate a failover switch. You can use this feature to return a failed unit to service, or to force an active unit offline for maintenance. If you are not using Stateful Failover, all active connections are dropped and must be reestablished by the clients after the failover occurs.

### Examples

The following example switches the standby unit to active:

```bash
> failover active
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>failover reset</td>
<td>Moves a device from a failed state to standby.</td>
</tr>
</tbody>
</table>
failover exec

To execute a command on a specific unit in a failover pair, use the `failover exec` command.

```
failover exec {active | standby | mate} cmd_string
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Specifies that the command is executed on the active unit in the failover pair.</td>
</tr>
<tr>
<td><code>cmd_string</code></td>
<td>The command to be executed. See the CLI help for supported commands.</td>
</tr>
<tr>
<td>mate</td>
<td>Specifies that the command is executed on the failover peer.</td>
</tr>
<tr>
<td>standby</td>
<td>Specifies that the command is executed on the standby unit in the failover pair.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use the `failover exec` command to send commands to a specific unit in a failover pair.

Output from the commands is displayed in the current terminal session, so you can use the `failover exec` command to issue `show` commands on a peer unit and view the results in the current terminal.

You must have sufficient privileges to execute a command on the local unit to execute the command on the peer unit.

**Limitations**

- Command completion and context help are not available for the commands in the `cmd_string` argument.
- You cannot use the `debug (undebug)` command with the `failover exec` command.
- If the standby unit is in the failed state, it can still receive commands from the `failover exec` command if the failure is due to a service card failure; otherwise, the remote command execution will fail.
- You cannot enter recursive `failover exec` commands, such as the `failover exec mate failover exec mate command`.
- Commands that require user input or confirmation must use the `/nonconfirm` option.

**Examples**

The following example uses the `failover exec` command to display the failover configuration of the failover peer. The command is executed on the primary unit, which is the active unit, so the information displayed is from the secondary, standby unit.

```
> failover exec mate show running-config failover
failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
```
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2

The following example uses the **failover exec** command to send the **show interface** command to the standby unit:

```plaintext
> failover exec standby show interface

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is 182546GB rev03, BW 1000 Mbps
  Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
  MAC address 000b.fc88.c290, MTU 1500
  IP address 192.168.5.111, subnet mask 255.255.255.0
  216 packets input, 27030 bytes, 0 no buffer
  Received 2 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 L2 decode drops
  284 packets output, 32124 bytes, 0 underruns
  0 output errors, 0 collisions
  0 late collisions, 0 deferred
  input queue (curr/max blocks): hardware (0/0) software (0/0)
  output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
  215 packets input, 23096 bytes
  0 packets dropped
  1 minute input rate 0 pkts/sec, 21 bytes/sec
  1 minute output rate 0 pkts/sec, 23 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec, 21 bytes/sec
  5 minute output rate 0 pkts/sec, 24 bytes/sec
  5 minute drop rate, 0 pkts/sec

Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is 182546GB rev03, BW 1000 Mbps
  Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
  MAC address 000b.fc88.c291, MTU 1500
  IP address 192.168.0.11, subnet mask 255.255.255.0
  214 packets input, 26902 bytes, 0 no buffer
  Received 1 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 L2 decode drops
  215 packets output, 27028 bytes, 0 underruns
  0 output errors, 0 collisions
  0 late collisions, 0 deferred
  input queue (curr/max blocks): hardware (0/0) software (0/0)
  output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
  214 packets input, 23050 bytes
  0 packets dropped
  1 minute input rate 0 pkts/sec, 21 bytes/sec
  1 minute output rate 0 pkts/sec, 21 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec, 21 bytes/sec
  5 minute output rate 0 pkts/sec, 21 bytes/sec
  5 minute drop rate, 0 pkts/sec

Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is 182546GB rev03, BW 1000 Mbps
  Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
  Description: LAN/STATE Failover Interface
  MAC address 000b.fc88.c293, MTU 1500
  IP address 10.0.5.2, subnet mask 255.255.255.0
  1991 packets input, 408734 bytes, 0 no buffer
  Received 1 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
1835 packets output, 254114 bytes, 0 underruns
0 output errors, 0 collisions
0 late collisions, 0 deferred
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/2) software (0/0)

Traffic Statistics for "failover":
1913 packets input, 345310 bytes
1755 packets output, 212452 bytes
0 packets dropped
1 minute input rate 1 pkts/sec, 319 bytes/sec
1 minute output rate 1 pkts/sec, 194 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 1 pkts/sec, 318 bytes/sec
5 minute output rate 1 pkts/sec, 192 bytes/sec
5 minute drop rate, 0 pkts/sec

...
failover reload-standby

To force the standby unit to reboot, use the `failover reload-standby` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command when your failover units do not synchronize. The standby unit restarts and resynchronizes to the active unit after it finishes booting.

**Examples**

The following example shows how to use the `failover reload-standby` command on the active unit to force the standby unit to reboot:

```
> failover reload-standby
```
failover reset

To restore a failed device to an unfailed state, use the `failover reset` command.

```
failover reset
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `failover reset` command allows you to change the failed unit to an unfailed state. The `failover reset` command can be entered on either unit, but we recommend that you always enter the command on the active unit. Entering the `failover reset` command at the active unit will “unfail” the standby unit.

You can display the failover status of the unit with the `show failover` command.

**Examples**

The following example shows how to change a failed unit to an unfailed state:

```
> failover reset
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show failover</td>
<td>Displays information about the failover status of the unit.</td>
</tr>
</tbody>
</table>
To transfer files from the common directory to a remote host via FTP, use the `file copy` command.

```
file copy host_name user_id path filename_1 [filename_2 ... filename_n]
```

**Syntax Description**
- `host_name` Specifies the name or IP address of the target remote host.
- `user_id` Specifies the user on the remote host.
- `path` Specifies the destination path on the remote host.
- `filename_1` through `filename_n` Specifies the names of the files to transfer from the common directory. If multiple file names are specified, they must be separated with blanks. This argument supports wildcards.

**Command Default**
This command transfers files only from the common directory where the system writes troubleshooting files.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
This example transfers all files in the common directory to the `/pub` directory on the remote host `sentinel` accessed via user `jdoe`:

```
> file copy sentinel jdoe /pub *
```
file delete

To erase files from the common directory, use the **file delete** command.

```
file delete  filename_1  [filename_2  ...  filename_n]
```

**Syntax Description**

- `filename_1` through `filename_n`: Specifies the names of the files to delete from the common directory. If multiple file names are specified, they must be separated with blanks. This argument supports wildcards.

**Command Default**

This command operates only on files in the common directory where the system writes troubleshooting files.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example deletes a single file:

```
> file delete 10.83.170.31-43235986-2363-11e6-b278-aff0a43948fe-troubleshoot.tar.gz
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file list</td>
<td>List files in the common directory.</td>
</tr>
<tr>
<td>file copy</td>
<td>Transfer files in the common directory via FTP.</td>
</tr>
<tr>
<td>file secure-copy</td>
<td>Transfer files in the common directory via SCP.</td>
</tr>
</tbody>
</table>
file list

To list the files in the common directory, use the file list command.

```
file list [filename_1 ... filename_n]
```

**Syntax Description**

- `filename_1` through `filename_n` Specifies the names of the files to list from the common directory. If multiple file names are specified, they must be separated with blanks. This argument supports wildcards.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command lists only files in the common directory where the system writes troubleshooting files. If no file names are specified, all files in the common directory are listed.

**Examples**

This example lists the contents of the common directory:

```
> file list
May 26 17:46 13747048 /core_1464284811_rackham-sfr.cisco.com_diskmanager_11.21145
Jun 27 20:36 1464696832 /core_1467059810_rackham-sfr.cisco.com_lina_6.21293
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file copy</td>
<td>Transfer files in the common directory via FTP.</td>
</tr>
<tr>
<td>file delete</td>
<td>Delete files from the common directory.</td>
</tr>
<tr>
<td>file secure-copy</td>
<td>Transfer files in the common directory via SCP.</td>
</tr>
</tbody>
</table>
file secure-copy

To transfer files from the common directory to a remote host via SCP, use the file secure-copy command.

```
file secure-copy  host_name  user_id  path  filename_1  [filename_2  ...  filename_n]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host_name</td>
<td>Specifies the name or IP address of the target remote host.</td>
</tr>
<tr>
<td>user_id</td>
<td>Specifies the user on the remote host.</td>
</tr>
<tr>
<td>path</td>
<td>Specifies the destination path on the remote host.</td>
</tr>
<tr>
<td>filename_1 through filename_n</td>
<td>Specifies the names of the files to transfer from the common directory. If multiple file names are specified, they must be separated with blanks. This argument supports wildcards.</td>
</tr>
</tbody>
</table>

**Command Default**

This command transfers files only from the common directory where the system writes troubleshooting files.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example transfers all files in the common directory to the /tmp directory on the remote host 101.123.31.1 accessed via user jdoe:

```
> file secure-copy 101.123.31.1 jdoe /tmp *
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file copy</td>
<td>Transfer files in the common directory via FTP.</td>
</tr>
<tr>
<td>file delete</td>
<td>Delete files from the common directory.</td>
</tr>
<tr>
<td>file list</td>
<td>List files in the common directory.</td>
</tr>
</tbody>
</table>
To perform a file system check and to repair corruptions, use the **fsck** command.

**fsck /noconfirm diskn:**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diskn:</td>
<td>Specifies the flash memory drive, where ( n ) is the drive number.</td>
</tr>
<tr>
<td>/noconfirm</td>
<td>Specifies that the command runs without prompting. This keyword is required.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The **fsck** command checks and tries to repair corrupt file systems. Use this command before trying more permanent procedures.

If the FSCK utility fixes an instance of disk corruption (due to power failure or abnormal shutdown, for example), it creates recovery files named FSCK\(xxx\).REC. These files can contain a fraction of a file or a whole file that was recovered while FSCK was running. In rare circumstances, you might need to inspect these files to recover data; generally, these files are not needed, and can be safely deleted.

**Note**
The FSCK utility runs automatically at startup, so you may see these recovery files even if you did not manually enter the **fsck** command.

**Examples**
The following example shows how to check the file system of the flash memory:

> fsck /noconfirm disk0:

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Removes all user-visible files.</td>
</tr>
<tr>
<td>erase</td>
<td>Deletes all files and formats the flash memory.</td>
</tr>
<tr>
<td>format</td>
<td>Formats the file system.</td>
</tr>
</tbody>
</table>
help

To display help information for a specified command, use the help command.

help {command | ?}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays all commands for which help is available.</td>
</tr>
<tr>
<td>command</td>
<td>Specifies the command for which to display the CLI help.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The help command displays help information about some commands. You can see help for an individual command by entering the help command followed by the command name. If you do not specify a command name and enter ? instead, all commands for which there is help are listed.

You can also get help by entering ? after entering a partial command. This shows you the valid parameters at that location in the command string.

Examples

The following example shows how to display help for the traceroute command:

```
> help traceroute
USAGE:
    traceroute <destination> [source <src_address|src_intf>] [numeric] [timeout <time>] [ttl <min-ttl> <max-ttl>] [probe <probes>] [port <port-value>] [use-icmp]
DESCRIPTION:
    traceroute  Print the route packets take to a network host
SYNTAX:
    destination  Address or hostname of destination
    src_address  Source address used in the outgoing probe packets
    src_intf    Interface through which the destination is accessible
    numeric     Do not resolve addresses to hostnames
    time        The time in seconds to wait for a response to a probe
    min-ttl     Minimum time-to-live value used in probe packets
    max-ttl     Maximum time-to-live value used in probe packets
    probes      The number of probes to send for each TTL value
    port-value  Base UDP destination port used in probes
    use-icmp    Use ICMP probes instead of UDP probes
```
history

To display the command line history for the current session, use the `history` command.

`history limit`

**Syntax Description**

| `limit` | The size of the history list in number of entries. To set the size to unlimited, that is, to see the full history, enter 0. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can also use the up arrow to scroll through past commands.

The history view includes sequence numbers for the order in which the commands were entered.

**Examples**

The following example shows the command history.

```plaintext
> history 0
  48 show environment
  49 show network-static-routes
  50 show network
  51 show running-config
  52 show service-policy
  53 show ntp
  54 show cpu
  55 show memory
  56 history 0
>
```
key chain

To configure rotating keys for authenticating IGP peers, use the **key chain** command. To remove the configuration, use the no form of the command.

```
key chain key-chain-name key-id key-string {0 | 8} key-string-text cryptographic-algorithm md5 [accept-lifetime [local | start-time] [duration {duration value | infinite | end-time}]] [send-lifetime [local | start-time] [duration {duration value | infinite | end-time}]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key-chain-name</td>
<td>The name for the key chain to be configured for OSPFv2 authentication.</td>
</tr>
<tr>
<td>key-id</td>
<td>The unique identifier in the key chain; the valid range being 1 to 255.</td>
</tr>
<tr>
<td>0</td>
<td>Specifies an unencrypted password will follow.</td>
</tr>
<tr>
<td>8</td>
<td>Specifies an encrypted password will follow.</td>
</tr>
<tr>
<td>key-string-text</td>
<td>The password for the key id. The string can be a plain text or an encrypted value.</td>
</tr>
<tr>
<td>md5</td>
<td>The supported cryptographic algorithm. Only md5 is supported.</td>
</tr>
<tr>
<td>accept-lifetime</td>
<td>(Optional) The time interval within which the device accepts the key during key exchange with another device. The accept lifetime, if not specified, is always active by default.</td>
</tr>
<tr>
<td>Send-lifetime</td>
<td>(Optional) The time interval within which the device sends the key during key exchange with another device. The send lifetime, if not specified, is always active by default.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use **key chain** command to configure the key chain to be used in OSPFv2 authentication for an interface. You must enter the **key id**, **key string**, and the **cryptographic-algorithm** command. Enter **accept** and **send lifetimes** to schedule the rotation of keys. The lifetime variables helps to handle secured key rollover. The device uses the lifetimes of keys to determine which keys in a keychain are active at any given point in time. When the lifetimes are not specified, the key chain authentication functions similar to that of MD5 authentication without time lines. Use the **no key chain** command to remove the configuration of the key chain.

**Examples**

The following example provides the output of the running key chain configuration:
> show running key chain
key chain CHAIN2
  key 1
  key-string KEY1CHAIN2
cryptographic-algorithm md5
  key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
cryptographic-algorithm md5
key chain CHAIN1
  key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
cryptographic-algorithm md5

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear configure keychain</td>
<td>Removes the key chains that are configured.</td>
</tr>
<tr>
<td>show key chain</td>
<td>Displays the configured key chains.</td>
</tr>
<tr>
<td>show running key chain</td>
<td>Displays the key chain details that is currently active.</td>
</tr>
</tbody>
</table>
logging savelog

To save the log buffer to flash memory, use the logging savelog command.

logging savelog  [savefile]

Syntax Description

| savefile | (Optional) The file name for the saved log. If you do not specify the file name, the system saves the log file using a default time-stamp format, as follows:
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LOG-YYYY-MM-DD-HHMMSS.TXT</td>
</tr>
<tr>
<td>where YYYY is the year, MM is the month, DD is the day of the month, and HHMMSS is the time in hours, minutes, and seconds.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Before you can save the log buffer to flash memory, you must enable logging to the buffer; otherwise, the log buffer never has data to be saved to flash memory. Configure buffer logging using the device manager, Firepower Management Center (remote) or Firepower Device Manager (local).

Note

The logging savelog command does not clear the buffer. To clear the buffer, use the clear logging buffer command.

Examples

The following example saves the log buffer to flash memory using the file name, latest-logfile.txt:

> logging savelog latest-logfile.txt
>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging buffer</td>
<td>Clears the log buffer of all syslog messages that it contains.</td>
</tr>
<tr>
<td>copy</td>
<td>Copies a file from one location to another, including to a TFTP or FTP server.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a file from the disk partition, such as saved log files.</td>
</tr>
</tbody>
</table>
logout

To exit from the CLI, use the **logout** command.

**logout**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **logout** command lets you log out of the device and end your CLI session. You can also use the **exit** command.

### Examples

The following example shows how to log out of the device:

> logout
memory caller-address

To configure a specific range of program memory for the call tracing, or caller PC, to help isolate memory problems, use the `memory caller-address` command. The caller PC is the address of the program that called a memory allocation primitive. To remove an address range, use the no form of this command.

```
memory caller-address startPC endPC
no memory caller-address
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>endPC</code></td>
<td>Specifies the end address range of the memory block.</td>
</tr>
<tr>
<td><code>startPC</code></td>
<td>Specifies the start address range of the memory block.</td>
</tr>
</tbody>
</table>

**Command Default**

The actual caller PC is recorded for memory tracing.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `memory caller-address` command to isolate memory problems to a specific block of memory.

In certain cases the actual caller PC of the memory allocation primitive is a known library function that is used at many places in the program. To isolate individual places in the program, configure the start and end program address of the library function, thereby recording the program address of the caller of the library function.

**Note**

The device might experience a temporary reduction in performance when caller-address tracing is enabled.

**Examples**

The following examples show the address ranges configured with the `memory caller-address` commands, and the resulting display of the `show memory caller-address` command:

```
> memory caller-address 0x00109d5c 0x00109e08
> memory caller-address 0x009b0ef0 0x009b0f14
> memory caller-address 0x00cf211c 0x00cf4464
> show memory caller-address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>memory profile enable</code></td>
<td>Enables the monitoring of memory usage (memory profiling).</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>memory profile text</td>
<td>Configures a text range of memory to profile.</td>
</tr>
<tr>
<td>show memory</td>
<td>Displays a summary of the maximum physical memory and current free memory available to the operating system.</td>
</tr>
<tr>
<td>show memory binsize</td>
<td>Displays summary information about the chunks allocated for a specific bin size.</td>
</tr>
<tr>
<td>show memory profile</td>
<td>Displays information about the memory usage (profiling) of the device.</td>
</tr>
<tr>
<td>show memory caller-address</td>
<td>Displays the address ranges configured on the device.</td>
</tr>
</tbody>
</table>
memory delayed-free-poisoner

Use the **memory delayed-free-poisoner** command to set parameters for the delayed free-memory poisoner tool. To enable the delayed free-memory poisoner tool, use the **memory delayed-free-poisoner enable** command. To disable the delayed free-memory poisoner tool, use the **no** form of this command. The delayed free-memory poisoner tool lets you monitor freed memory for changes after it has been released by an application.

```
memory delayed-free-poisoner enable

no memory delayed-free-poisoner enable
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Start operation of the delayed free-memory poisoner tool.</td>
</tr>
<tr>
<td>desired-fragment-count frag_count</td>
<td>Set the number of memory fragments to keep in the poisoner’s queue. Legal values range from 0 to 8192; the default is 16</td>
</tr>
<tr>
<td>desired-fragment-size frag-size</td>
<td>Set the size in bytes of the contiguous free memory fragments to keep in the poisoner’s queue. Legal values range from 0 to 268435456; the default is 102400.</td>
</tr>
<tr>
<td>threshold heap_use_percent</td>
<td>Set the percentage threshold of system memory use at which the system will release memory from the poisoner’s queue, ranging from 0 to 100. The default is 100.</td>
</tr>
<tr>
<td>validate</td>
<td>Forces validation of all elements in the delayed-free-poisoner queue.</td>
</tr>
<tr>
<td>watchdog-percent watchdog_limit</td>
<td>Set the watchdog limit as a percentage of the watchdog threshold, which is 15 seconds. Values range from 10 to 100. The default is 50.</td>
</tr>
</tbody>
</table>

**Command Default**

The **memory delayed-free-poisoner enable** command is disabled by default.

The default **desired-fragment-count** is 16.

The default **desired-fragment-size** is 102400.

The default **watchdog-percent** is 50.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enabling the delayed free-memory poisoner tool has a significant impact on memory usage and system performance. The command should be used only under the supervision of the Cisco Technical Assistance Center. It should not be run in a production environment during heavy system usage.

When you enable this tool, requests to free memory by the applications running on the device are written to a FIFO queue. As each request is written to the poisoner’s queue, each associated byte of memory that is not required by lower-level memory management is “poisoned” by being written with the value 0xcc.

The freed memory requests remain in the queue until more memory is required by an application than is in the system free memory pool. When more memory is needed, the poisoner seeks at least
**desired-fragment-count** memory buffers of **desired-fragment-size** bytes in its queue, pulls that memory from the queue, and validates it. You can tune the time it takes the poisoner to satisfy large memory requests by changing the values for **desired-fragment-size** and **desired-fragment-count**.

If the memory is unmodified, it is returned to the system free memory pool and the poisoner reissues the memory request from the application that made the initial request. The process repeats until enough memory for the requesting application is freed.

If the poisoned memory has been modified, then the system forces a crash and produces diagnostic output which can be used to determine the cause of the crash.

The delayed free poisoner includes a watchdog mechanism to prevent processes from excessive resource usage. The watchdog threshold is 15 seconds, and when a process executes continuously for that time without relinquishing the CPU, the poisoner forces a system crash.

You can tune the watchdog behavior by setting the watchdog limit, which indicates a percentage of the 15 second watchdog threshold; the default is 50%. Therefore when the delayed free poisoner is active, by default if a process executes continuously for 7.5 seconds without relinquishing the CPU, further memory allocation requests from that process fail until the process is rescheduled. You can tune this behavior by changing the value of the watchdog limit.

To guard against excessive memory fragmentation and reduce system CPU load, you can set a percentage **threshold** of free memory usage at which the poisoner automatically releases memory from its queue to the system memory pool. (By default, the poisoner does not release memory from its queue until system memory has been exhausted.)

The delayed free-memory poisoner tool periodically performs validation on all of the elements of the queue automatically. You can also start validation manually using the **memory delayed-free-poisoner validate** command. If an element contains unexpected values, then the system forces a crash and produces diagnostic output to determine the cause of the crash. If no unexpected values are encountered, the elements remain in the queue and are processed normally by the tool; the **memory delayed-free-poisoner validate** command does not cause the memory in the queue to be returned to the system memory pool.

The **no** form of the command causes all of the memory referenced by the requests in the queue to be returned to the free memory pool without validation and any statistical counters to be cleared.

### Examples

The following example enables the delayed free-memory poisoner tool:

```
> memory delayed-free-poisoner enable
```

The following is sample output when the delayed free-memory poisoner tool detects illegal memory reuse:

```
delayed-free-poisoner validate failed because a data signature is invalid at delayfree.c:328.
  heap region: 0x025b1cacf-0x025b1d53 (184 bytes)
  memory address: 0x025b1cb4
  byte offset: 8
  allocated by: 0x0060b812
  freed by: 0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80: ef cd 1c a1 e1 00 00 00 | ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02 | #.........`h.`.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02 | ..........l&[.
```

Cisco Firepower Threat Defense Command Reference
An internal error occurred. Specifically, a programming assertion was violated. Copy the error message exactly as it appears, and get the output of the show version command and the contents of the configuration file. Then call your technical support representative.

```
assertion "0" failed: file "delayfree.c", line 191
```

The following table describes the significant portion of the output.

### Table 1: Illegal Memory Usage Output Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>heap region</td>
<td>The address region and size of the region of memory available for use by the requesting application. This is not the same as the requested size, which may be smaller given the manner in which the system may parcel out memory at the time the memory request was made.</td>
</tr>
<tr>
<td>memory address</td>
<td>The location in memory where the fault was detected.</td>
</tr>
<tr>
<td>byte offset</td>
<td>The byte offset is relative to the beginning of the heap region and can be used to find the field that was modified if the result was used to hold a data structure starting at this address. A value of 0 or that is larger than the heap region byte count may indicate that the problem is an unexpected value in the lower level heap package.</td>
</tr>
<tr>
<td>allocated by/freed by</td>
<td>Instruction addresses where the last malloc/calloc/realloc and free calls where made involving this particular region of memory.</td>
</tr>
<tr>
<td>Dumping...</td>
<td>A dump of one or two regions of memory, depending upon how close the detected fault was to the beginning of the region of heap memory. The next eight bytes after any system heap header is the memory used by this tool to hold a hash of various system header values plus the queue linkage. All other bytes in the region until any system heap trailer is encountered should be set to 0xcc.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear memory delayed-free-poisoner</td>
<td>Clears the delayed free-memory poisoner tool queue and statistics.</td>
</tr>
<tr>
<td>show memory delayed-free-poisoner</td>
<td>Displays a summary of the delayed free-memory poisoner tool queue usage.</td>
</tr>
</tbody>
</table>
memory logging

To enable memory logging, use the `memory logging` command. To disable memory logging, use the `no` form of this command.

```
memory logging 1024-4194304 [wrap [size [1-2147483647] | process process-name]]
```

```
no memory logging
```

**Syntax Description**

- `1024-4194304` Specifies the number of logging entries in the memory logging buffer. This is the only required argument to specify.

- `process process-name` Specifies the process to monitor.

**Note** The Checkheaps process is completely ignored as a process because it uses the memory allocator in a non-standard way.

- `size 1-2147483647` Specifies the size and number of entries to monitor.

- `wrap` Save the buffer when it wraps. It can only be saved once. If it wraps multiple times, it can be overwritten. When the buffer wraps, a trigger is sent to the event manager to enable saving of the data.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To change memory logging parameters, you must disable it, then reenable it. Use the `show memory logging` command to view the log.

**Examples**

The following example enables memory logging:

```
> memory logging 202980
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show memory logging</td>
<td>Displays memory logging results.</td>
</tr>
</tbody>
</table>
memory profile enable

To enable the monitoring of memory usage (memory profiling), use the **memory profile enable** command. To disable memory profiling, use the **no** form of this command.

```
memory profile enable [peak peak_value]
no memory profile enable [peak peak_value]
```

**Syntax Description**

- **peak peak_value**
  
  Specifies the memory usage threshold at which a snapshot of the memory usage is saved to the peak usage buffer. The contents of this buffer could be analyzed at a later time to determine the peak memory needs of the system.

**Command Default**

Memory profiling is disabled by default.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before enabling memory profiling, you must first configure a memory text range to profile with the **memory profile text** command.

Some memory is held by the profiling system until you enter the **clear memory profile** command. See the output of the **show memory profile status** command.

*Note*

The device might experience a temporary reduction in performance when memory profiling is enabled.

**Examples**

The following example enables memory profiling:

```
> memory profile enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory profile text</td>
<td>Configures a text range of memory to profile.</td>
</tr>
<tr>
<td>show memory profile</td>
<td>Displays information about the memory usage (profiling) of the device.</td>
</tr>
</tbody>
</table>
To configure a program text range of memory to profile, use the `memory profile text` command. To disable, use the no form of this command.

```plaintext
memory profile text {startPC endPC | all} resolution
no memory profile text {startPC endPC | all} resolution
```

### Syntax Description

- `all` Specifies the entire text range of the memory block.
- `endPC` Specifies the end text range of the memory block.
- `resolution` You must set the resolution of tracing for the source text region, from 1-44582263.
- `startPC` Specifies the start text range of the memory block.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

For a small text range, a resolution of “4” normally traces the call to an instruction. For a larger text range, a coarse resolution is probably enough for the first pass and the range could be narrowed down to a set of smaller regions in the next pass.

After entering the text range with the `memory profile text` command, you must then enter the `memory profile enable` command to begin memory profiling. Memory profiling is disabled by default.

**Note**

The device might experience a temporary reduction in performance when memory profiling is enabled.

### Examples

The following example shows how to configure a text range of memory to profile, with a resolution of 100.

```plaintext
> memory profile text all 100
```

The following example displays the configuration of the text range and the status of memory profiling (OFF):

```plaintext
> show memory profile status
InUse profiling: OFF
Peak profiling: OFF
Memory used by profile buffers: 0 bytes
Profile: 0x00007efc3e0227a8-0x00007efc40aa1f8e(00000100)
```
To begin memory profiling, you must enter the `memory profile enable` command. Memory profiling is disabled by default.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear memory profile</td>
<td>Clears the buffers held by the memory profiling function.</td>
</tr>
<tr>
<td>memory profile enable</td>
<td>Enables the monitoring of memory usage (memory profiling).</td>
</tr>
<tr>
<td>show memory profile</td>
<td>Displays information about the memory usage (profiling) of the device.</td>
</tr>
</tbody>
</table>
memory tracking

To enable the tracking of heap memory request, use the memory tracking command. To disable memory tracking, use the no form of this command.

```
memory tracking (enable | allocates-by-threshold min_allocates | bytes-threshold min_bytes | filter-from-address-pool address)
no memory tracking enable
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable memory tracking.</td>
</tr>
<tr>
<td>allocates-by-threshold min_allocates</td>
<td>Address pool entries for callers must make at least this many allocation calls to be included, from 0-4294967295.</td>
</tr>
<tr>
<td>bytes-threshold min_bytes</td>
<td>Address pool entries for callers must consume at least this many bytes of memory to be included, from 0-4294967295.</td>
</tr>
</tbody>
</table>
| filter-from-address-pool address | Exclude address pool entries at this address. To determine an address, first enable tracking, then use show memory tracking address. Look for the “allocated by” address in the “memory tracking address pool” listing. For example, if you see the following:

...allocated by 0x00007efc3f80e508

You can exclude it using:

```
filter-from-address-pool 0x00007efc3f80e508
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example enables tracking heap memory requests:

```
> memory tracking enable
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear memory tracking</td>
<td>Clears all currently gathered information.</td>
</tr>
<tr>
<td>show memory tracking</td>
<td>Shows memory tracking results.</td>
</tr>
</tbody>
</table>
more

To display the contents of a file, use the more command.

```
```

**Syntax Description**

- `/ascii` (Optional) Displays a binary file in binary mode and an ASCII file in binary mode.
- `/binary` (Optional) Displays any file in binary mode.
- `/ebcdic` (Optional) Displays binary files in EBCDIC.
- `/disk0:` (Optional) Displays a file on the internal Flash memory.
- `/disk1:` (Optional) Displays a file on the external Flash memory card.
- `/filename` Specifies the name of the file to display.
- `/flash:` (Optional) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series adaptive security appliance, the `flash` keyword is aliased to `/disk0`.
- `/ftp:` (Optional) Displays a file on an FTP server.
- `/http:` (Optional) Displays a file on a website.
- `/https:` (Optional) Displays a file on a secure website.
- `/tftp:` (Optional) Displays a file on a TFTP server.

**Command Default**

ASCII mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `system support view-files` command is a better option for finding and viewing log files.

**Examples**

The following example shows how to display the contents of a local file named “test.cfg”:

```
> more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
```
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
interface outside
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179 location my_context, USA
ciscoasa test
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
end

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Changes to the specified directory.</td>
</tr>
<tr>
<td>pwd</td>
<td>Displays the current working directory.</td>
</tr>
<tr>
<td>system support</td>
<td>Find and view the contents of log files.</td>
</tr>
</tbody>
</table>
nslookup

To look up the IP address for a fully-qualified domain name, or the reverse, use the nslookup command.

```
nslookup {hostname | ip_address}
```

**Syntax Description**

- **hostname**: The fully-qualified domain name of a host whose IP address you are looking up. For example, www.example.com.
- **ip_address**: The IP address of a host whose fully-qualified domain name you are looking up.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Some commands that allow fully-qualified domain names cannot use the DNS servers configured for the management interface to look up the IP address for the name. If you do not have DNS servers configured for commands that go through the data interfaces, use the nslookup command to determine the IP address, then use the IP address in the command.

The nslookup command is also useful in determining the fully-qualified domain name for a given IP address.

**Examples**

The following example looks up the IP address for www.cisco.com. The initial Server and Address information shows the DNS server (which could be a fully-qualified domain name), IP address, and port. (The addresses in this example are faked.) The following information shows the canonical (real) host name and IP address for the name you entered.

```
> nslookup www.cisco.com
Server: 10.102.6.247
Address: 10.102.6.247#53

Name: origin-www.cisco.com
Address: 173.37.145.84
```

The following example shows how to do a reverse lookup and determine a hostname for an IP address. The initial information is for the DNS server used. The mapped hostname is indicated by the name = field.

```
> nslookup 173.37.145.84
Server: 10.102.6.247
Address: 10.102.6.247#53

84.145.37.173.in-addr.arpa name = www2.cisco.com.
```
To enable packet tracing capabilities for troubleshooting by specifying the 5-tuple to test firewall rules, use the `packet-tracer` command. For clarity, the syntax is shown separately for ICMP, TCP/UDP, and IP packet modeling.

```
packet-tracer input ifc_name icmp { sip | user username } type code [ident] [dip | fqdn fqdn-string] [detailed] [xml]
```

```
packet-tracer input ifc_name [ tcp | udp ] { sip | user username } sport [dip | fqdn fqdn-string] [detailed] [xml]
```

```
packet-tracer input ifc_name rawip { sip | user username } protocol [dip | fqdn fqdn-string] [detailed] [xml]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>code</code></td>
<td>Specifies the ICMP code for an ICMP packet trace.</td>
</tr>
<tr>
<td><code>detailed</code></td>
<td>(Optional) Provides detailed trace results information.</td>
</tr>
<tr>
<td><code>dip</code></td>
<td>Specifies the destination IPv4 or IPv6 address for the packet trace.</td>
</tr>
<tr>
<td><code>dport</code></td>
<td>Specifies the destination port for a TCP/UDP/SCTP packet trace.</td>
</tr>
<tr>
<td><code>fqdn fqdn-string</code></td>
<td>Specifies the fully qualified domain name of the host. Supports the FQDN for IPv4 only.</td>
</tr>
<tr>
<td><code>icmp</code></td>
<td>Specifies the protocol to use is ICMP.</td>
</tr>
<tr>
<td><code>ident</code></td>
<td>(Optional.) Specifies the ICMP identifier for an ICMP packet trace.</td>
</tr>
<tr>
<td><code>input ifc_name</code></td>
<td>Specifies the name of the source interface on which to trace the packets.</td>
</tr>
<tr>
<td><code>protocol</code></td>
<td>Specifies the protocol number for raw IP packet tracing, 0-255.</td>
</tr>
<tr>
<td><code>rawip</code></td>
<td>Specifies the protocol to use is raw IP.</td>
</tr>
<tr>
<td><code>sip</code></td>
<td>Specifies the source IPv4 or IPv6 address for the packet trace.</td>
</tr>
<tr>
<td><code>sport</code></td>
<td>Specifies the source port for a TCP/UDP/SCTP packet trace.</td>
</tr>
<tr>
<td><code>tcp</code></td>
<td>Specifies the protocol to use is TCP.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>Specifies the ICMP type for an ICMP packet trace.</td>
</tr>
<tr>
<td><code>udp</code></td>
<td>Specifies the protocol to use is UDP.</td>
</tr>
<tr>
<td><code>user username</code></td>
<td>Specifies the user identity in the format of domain\user if you want to specify the user as the source IP address. The most recently mapped address for the user (if any) is used in the trace.</td>
</tr>
<tr>
<td><code>xml</code></td>
<td>(Optional) Displays the trace results in XML format.</td>
</tr>
</tbody>
</table>
In addition to capturing packets, it is possible to trace the lifespan of a packet through the Firepower Threat Defense device to see if it is behaving as expected. The `packet-tracer` command enables you to do the following:

- Debug all packet drops in production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet along with the CLI lines that caused the rule addition.
- Show a time line of packet changes in a data path.
- Inject tracer packets into the data path.

The `packet-tracer` command provides detailed information about the packets and how they are processed by the Firepower Threat Defense device. If a command from the configuration did not cause the packet to drop, the `packet-tracer` command provides information about the cause in an easily readable format. For example if a packet was dropped because of an invalid header validation, the following message appears: “packet dropped due to bad ip header (reason).”

**Examples**

The following example traces a TCP packet for the HTTP port from 10.100.10.10 to 10.100.11.11. The result indicates that the packet will be dropped by the implicit deny access rule.

```
> packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11 80
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture</td>
<td>Captures packet information, including trace packets.</td>
</tr>
<tr>
<td>show capture</td>
<td>Displays the capture configuration when no options are specified.</td>
</tr>
</tbody>
</table>
perfmon

To display performance information at the console, use the `perfmon` command.

```
perfmon { verbose | interval seconds | settings }
```

**Syntax Description**

| verbose | Displays performance monitor information at the console. The default is to not display information, which is shown as “quiet” in the perfmon settings.
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>interval seconds</td>
<td>Specifies the number of seconds before the performance display is refreshed on the console.</td>
</tr>
<tr>
<td>settings</td>
<td>Displays the interval and whether perfmon is quiet or verbose.</td>
</tr>
</tbody>
</table>

**Command Default**

The default interval is 120 seconds.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `perfmon` command allows you to monitor the performance of the device. Use the `show perfmon` command to display the information immediately.

Use the `perfmon verbose` command to display the information on the console each interval.

The information appears automatically only if you are actually connected to the CLI on the Console port, or if you are in the Diagnostic CLI (`system support diagnostic-cli`). If you are in the CLI on a different port, including the management interface, use the `show console-output` command to see the automatically-generated information. Alternatively, do not use this command, and simply use the `show perfmon` command directly.

We recommend you use this command in the Diagnostic CLI only.

**Note**

You cannot turn off `verbose` from the regular CLI. Instead, you must turn it off from Privileged EXEC mode in the Diagnostic CLI. See the examples section.

**Examples**

This example shows how to display the performance monitor statistics every 120 seconds on the console. In the output, the “Fixup” statistics refer to the related protocol inspection engine.

```
> perfmon verbose
> perfmon settings
interval: 120 (seconds)
verbose
> show console-output
...
Message #109 :
```
The following example shows how to turn off verbose mode. You must do so from the Diagnostic CLI.

> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '? for a list of available commands.

firepower> enable
Password: <Press return, do not enter a password>

firepower# perfmon quiet

firepower# perfmon settings
interval: 120 (seconds)
quiet
firepower# <Press Ctrl+a, d>

Console connection detached.
> perfmon settings
interval: 120 (seconds)
quiet

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show perfmon</td>
<td>Displays performance information.</td>
<td></td>
</tr>
</tbody>
</table>
pigtail commands

Only use **pigtail** commands under the direction of the Cisco Technical Assistance Center.

If you want to view logs as they are written, use the **tail-logs** command instead of **pigtail**.

---

**Caution**

Do not leave the pigtail process running as it can cause high disk usage. This process may also interfere with policy deployment if it is running during deployment. For information on how to stop the pigtail process, contact the Cisco Technical Assistance Center.
ping

To test connectivity from a specified interface to an IP address, use the ping command. The parameters available differ for regular ICMP-based ping, TCP ping, and a “system” ping. Also, system pings are from the management interface, whereas the other types of ping go through the data interfaces. Be sure to use the correct type of ping for your tests.

```
ping [interface if_name] host [repeat count] [timeout seconds] [data pattern] [size bytes] [validate]
ping tcp [interface if_name] host port [repeat count] [timeout seconds] [source host port]
ping system host
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>data pattern</code></td>
<td>(Optional, ICMP only.) Specifies the 16-bit data pattern in hexadecimal format, from 0 to FFFF. The default is 0xabcd.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Specifies the IPv4 address or name of the host to ping. For ICMP pings, you can also specify an IPv6 address. IPv6 is not supported for TCP or system pings. Whether a ping can use a fully-qualified domain name, such as <a href="http://www.example.com">www.example.com</a>, depends on the availability of a DNS server to resolve the name. The system pings use the DNS servers for the management interface, but other types of ping do not use the management DNS servers. You must configure DNS for the data interfaces for non-system hostname pings to work. If ping cannot resolve a hostname, use nslookup to determine the IP address associated with the name, and then ping the IP address.</td>
</tr>
<tr>
<td><code>interface if_name</code></td>
<td>(Optional) For ICMP, this is the name of the interface through which the host is accessible. If not supplied, then the host is resolved to an IP address and the routing table is consulted to determine the destination interface. For TCP, this is the input interface through which the source sends SYN packets.</td>
</tr>
<tr>
<td><code>port</code></td>
<td>(TCP only.) Specifies the TCP port number for the host you are pinging, 1-65535.</td>
</tr>
<tr>
<td><code>repeat count</code></td>
<td>(Optional) Specifies the number of times to repeat the ping request. The default is 5.</td>
</tr>
<tr>
<td><code>size bytes</code></td>
<td>(Optional, ICMP only.) Specifies the datagram size in bytes. The default is 100.</td>
</tr>
<tr>
<td><code>source host port</code></td>
<td>(Optional, TCP only.) Specifies a certain IP address and port to send the ping from (Use port = 0 for a random port).</td>
</tr>
<tr>
<td><code>system</code></td>
<td>Ping the host through the management interface. Unlike pings through the data interfaces, there is no default count for system pings. The ping continues until you stop it using Ctrl+c.</td>
</tr>
<tr>
<td><code>tcp</code></td>
<td>(Optional) Tests a connection over TCP (the default is ICMP). A TCP ping sends SYN packets and considers the ping successful if the destination sends a SYN-ACK packet. You can also have at most 2 concurrent TCP pings running at a time.</td>
</tr>
</tbody>
</table>
timeout seconds  (Optional) Specifies the number of seconds of the timeout interval. The default is 2 seconds.

validate  (Optional, ICMP only.) Validates reply data.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The ping command allows you to determine if the device has connectivity or if a host is available on the network.

When using regular ICMP-based ping, ensure that you do not have ICMP rules that prohibit these packets (if you do not use ICMP rules, all ICMP traffic is allowed).

When using TCP ping, you must ensure that access policies allow TCP traffic on the ports you specify.

This configuration is required to allow the device to respond and accept messages generated from the ping command. The ping command output shows if the response was received. If a host is not responding after you enter the ping command, a message similar to the following appears:

```
> ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
??????
Success rate is 0 percent (0/5)
```

Use the show interface command to ensure that the device is connected to the network and is passing traffic. The address of the specified interface name is used as the source address of the ping.

Examples

The following example shows how to determine if an IP address is accessible through a data interface. Because no interface is specified, the routing table is used to determine how to get to the address.

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following examples use TCP ping to determine if a host is accessible through a data interface.

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21 from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
> ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21 from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!!
```
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms

The following example does a system ping to determine if www.cisco.com is accessible through the management interface. You must use Ctrl+c to stop the ping (indicated by ^C in the output).

```plaintext
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nslookup</td>
<td>Perform a DNS lookup for a hostname or IP address.</td>
</tr>
<tr>
<td>show interface</td>
<td>Displays information about the interface configuration.</td>
</tr>
</tbody>
</table>
pmtool commands

Only use `pmtool` commands under the direction of the Cisco Technical Assistance Center.
To reboot the device, use the `reboot` command.

```
reboot
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

```
> reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': yes

Broadcast message from root@firepower

The system is going down for reboot NOW!
...```
redundant-interface

To set which member interface of a redundant interface is active, use the `redundant-interface` command.

`redundant-interface redundant number active-member physical_interface`

**Syntax Description**

| active-member | Sets the active member. Use the show interface command to see available physical interface names, such as GigabitEthernet0/0. Both member interfaces must be the same physical type. |
| redundant number | Specifies the redundant interface ID, such as `redundant 1`. Numbers are 1-8. |

**Command Default**

By default, the active interface is the first member interface listed in the configuration, if it is available.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Create redundant interfaces in the device manager. When you create the redundant interface, you specify which is primary. Use this command to change which interface is active during run time.

To view which interface is active, enter the following command:

`show interface redundant number detail | grep Member`

For example:

`show interface redundant1 detail | grep Member`

Members GigabitEthernet0/3(Active), GigabitEthernet0/2

**Examples**

The following example changes the active interface for the redundant1 interface.

`redundant-interface redundant 1 active-member gigabitethernet0/2`

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear interface</td>
<td>Clears counters for the <code>show interface</code> command.</td>
</tr>
<tr>
<td>show interface</td>
<td>Displays the runtime status and statistics of interfaces.</td>
</tr>
</tbody>
</table>
**restore**

To restore configuration backed up locally from a Firepower Threat Defense device being managed by a Firepower Management Center, use the `restore` command. To restore a backup saved to a remote location, specify additional parameters for location of the backup file and username.

```
restore remote-manager-backup [ backup tar-file | location [ scp-hostname username filepath backup tar-file ] ]
```

**Syntax Description**

- `remote-manager-backup backup tar-file` Restore a local backup created by the Firepower Management Center. The local backup file is saved on the Firepower Threat Defense device.

- `remote-manager-backup location scp-hostname username filepath backup tar-file` Restore a remote backup created by the Firepower Management Center. The remote backup is saved at a user-configured location, accessible by an SCP server and identified by the hostname, username and file path.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `restore` command restores the Firepower Threat Defense system files, Snort DB tables and the LINA running configuration on the new/replacement Firepower Threat Defense. The `restore` command also ensures that the existing LINA running configuration on the Firepower Threat Defense device is deleted before the actual restore operation proceeds. This ensures that the Firepower Threat Defense device carries only the configurations present at the time the backup was taken. All device configurations except the serial number of the replacement device, will be replaced after a successful restore operation.

The restore operation ensures that the connection between the replacement/new Firepower Threat Defense device and the original Firepower Management Center is re-established using the universally unique identifier (UUID), assigned to the original device. After successful restore, the Firepower Management Center marks all the policies of the device as out-of-date so that any configuration changes on the Firepower Management Center that may affect the replacement Firepower Threat Defense are deployed to it, when the device replacement procedure is complete. This ensures that the new Firepower Threat Defense and Firepower Management Center configurations are in sync.

**Examples**

The following example shows a restore operation from a local backup file:

```
> restore remote-manager-backup 10.10.1.168_PRIMARY_20180614055906.tar
```

The following example shows a restore operation from a remote backup file:

```
> restore remote-manager-backup location 10.106.140.100 admin /Volume/home/admin 10.10.1.168_PRIMARY_20180614055906.tar
```
PART II

S Commands

• sa - show a, on page 295
• show b, on page 353
• show c, on page 415
• show d - show h, on page 503
• show i, on page 571
• show j - show o, on page 683
• show p - show r, on page 773
• show s - sz, on page 829
• sftunnel-status, on page 297
• show aaa-server, on page 300
• show access-control-config, on page 303
• show access-list, on page 306
• show alarm settings, on page 310
• show app-agent heartbeat, on page 311
• show arp, on page 312
• show arp-inspection, on page 313
• show arp statistics, on page 314
• show as-path-access-list, on page 316
• show asp cluster counter, on page 317
• show asp dispatch, on page 318
• show asp drop, on page 319
• show asp event, on page 320
• show asp inspect-dp egress-optimization, on page 321
• show asp inspect-dp snapshot, on page 323
• show asp inspect-dp snort, on page 324
• show asp inspect-dp snort counters, on page 326
• show asp inspect-dp snort counters summary, on page 328
• show asp inspect-dp snort queues, on page 329
• show asp inspect-dp snort queue-exhaustion, on page 331
• show asp load-balance, on page 332
• show asp multiprocessor accelerated- features, on page 334
• show asp overhead, on page 335
• show asp packet-profile, on page 336
• show asp table arp, on page 338
• show asp table classify, on page 339
• show asp table cluster chash-table, on page 342
• show asp table interfaces, on page 343
• show asp table routing, on page 344
• show asp table socket, on page 346
• show asp table vpn-context, on page 348
• show asp table zone, on page 350
• show audit-log, on page 351
sftunnel-status

To view the status of the connection (tunnel) between the device and the managing Firepower Management Center, use the `sftunnel-status` command.

**sftunnel-status**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `sftunnel-status` command to view the status of the connection between the device and the managing Firepower Management Center. If you are using the local manager, Firepower Device Manager, this command does not provide any information.

Status information includes the following sections:

- SFTUNNEL Status—When the connection was established and information about management interfaces used in the connection.
- RUN STATUS—IP address, encryption, and registration status information.
- PEER INFO—Information about the Firepower Management Center and its connection to this device. This section also includes statistics blocks for several types of messages that might be transmitted between the systems for various services, including Identity, Health Events, RPC, NTP, IDS, Malware Lookup, CSM_CCM (used for configuring the device), EStreamer, UE Channel, and FSTREAM.
- RPC status.

**Examples**

The following is sample output from the `sftunnel-status` command.

```
> sftunnel-status
   Both IPv4 and IPv6 connectivity is supported
   Broadcast count = 2
   Reserved SSL connections: 0
   Management Interfaces: 1
       br1 (control events) 10.83.57.37,2001:420:2710:2556:1:0:0:37

******************************
**RUN STATUS****10.83.57.41*************
   Cipher used = AES256-GCM-SHA384 (strength:256 bits)
   ChannelA Connected: Yes, Interface br1
   Cipher used = AES256-GCM-SHA384 (strength:256 bits)
   ChannelB Connected: Yes, Interface br1
   Registration: Completed.
   IPv4 Connection to peer '10.83.57.41' Start Time: Tue Oct 11 21:46:00 2016

PEER INFO:
   sw_version 6.2.0
```
sw_build 2007
Management Interfaces: 1
eth0 (control events) 10.83.57.41,2001:420:2556:1:0:0:41
Peer channel Channel-A is valid type (CONTROL), using 'br1',
connected to '10.83.57.41' via '10.83.57.37'
Peer channel Channel-B is valid type (EVENT), using 'br1',
connected to '10.83.57.41' via '10.83.57.37'

TOTAL TRANSMITTED MESSAGES <3> for Identity service
RECEIVED MESSAGES <2> for Identity service
SEND MESSAGES <1> for Identity service
HALT REQUEST SEND COUNTER <0> for Identity service
STORED MESSAGES for Identity service (service 0/peer 0)
STATE <Process messages> for Identity service
REQUESTED FOR REMOTE <Process messages> for Identity service
REQUESTED FROM REMOTE <Process messages> for Identity service

TOTAL TRANSMITTED MESSAGES <2760> for Health Events service
RECEIVED MESSAGES <1380> for Health Events service
SEND MESSAGES <1380> for Health Events service
HALT REQUEST SEND COUNTER <0> for Health Events service
STORED MESSAGES for Health service (service 0/peer 0)
STATE <Process messages> for Health Events service
REQUESTED FOR REMOTE <Process messages> for Health Events service
REQUESTED FROM REMOTE <Process messages> for Health Events service

TOTAL TRANSMITTED MESSAGES <656> for RPC service
RECEIVED MESSAGES <328> for RPC service
SEND MESSAGES <328> for RPC service
HALT REQUEST SEND COUNTER <0> for RPC service
STORED MESSAGES for RPC service (service 0/peer 0)
STATE <Process messages> for RPC service
REQUESTED FOR REMOTE <Process messages> for RPC service
REQUESTED FROM REMOTE <Process messages> for RPC service

TOTAL TRANSMITTED MESSAGES <25131> for IP(NTP) service
RECEIVED MESSAGES <13532> for IP(NTP) service
SEND MESSAGES <11599> for IP(NTP) service
HALT REQUEST SEND COUNTER <0> for IP(NTP) service
STORED MESSAGES for IP(NTP) service (service 0/peer 0)
STATE <Process messages> for IP(NTP) service
REQUESTED FOR REMOTE <Process messages> for IP(NTP) service
REQUESTED FROM REMOTE <Process messages> for IP(NTP) service

TOTAL TRANSMITTED MESSAGES <2890> for IDS Events service
RECEIVED MESSAGES <1445> for service IDS Events service
SEND MESSAGES <1445> for IDS Events service
HALT REQUEST SEND COUNTER <0> for IDS Events service
STORED MESSAGES for IDS Events service (service 0/peer 0)
STATE <Process messages> for IDS Events service
REQUESTED FOR REMOTE <Process messages> for IDS Events service
REQUESTED FROM REMOTE <Process messages> for IDS Events service

TOTAL TRANSMITTED MESSAGES <4> for Malware Lookup Service service
RECEIVED MESSAGES <1> for Malware Lookup Service service
SEND MESSAGES <3> for Malware Lookup Service service
HALT REQUEST SEND COUNTER <0> for Malware Lookup Service service
STORED MESSAGES for Malware Lookup Service service (service 0/peer 0)
STATE <Process messages> for Malware Lookup Service service
REQUESTED FOR REMOTE <Process messages> for Malware Lookup Service service
REQUESTED FROM REMOTE <Process messages> for Malware Lookup Service service

TOTAL TRANSMITTED MESSAGES <372> for CSM_CCM service
RECEIVED MESSAGES <186> for CSM_CCM service
SEND MESSAGES <186> for CSM_CCM service
HALT REQUEST SEND COUNTER <0> for CSM_CCM service
STORED MESSAGES for CSM_CCM (service 0/peer 0)
STATE <Process messages> for CSM_CCM service
REQUESTED FOR REMOTE <Process messages> for CSM_CCM service
REQUESTED FROM REMOTE <Process messages> for CSM_CCM service

TOTAL TRANSMITTED MESSAGES <2907> for EStreamer Events service
RECEIVED MESSAGES <1453> for service EStreamer Events service
SEND MESSAGES <1454> for EStreamer Events service
HALT REQUEST SEND COUNTER <0> for EStreamer Events service
STORED MESSAGES for EStreamer Events service (service 0/peer 0)
STATE <Process messages> for EStreamer Events service
REQUESTED FOR REMOTE <Process messages> for EStreamer Events service
REQUESTED FROM REMOTE <Process messages> for EStreamer Events service

Priority UE Channel 1 service

TOTAL TRANSMITTED MESSAGES <2930> for UE Channel service
RECEIVED MESSAGES <11> for UE Channel service
SEND MESSAGES <2919> for UE Channel service
HALT REQUEST SEND COUNTER <0> for UE Channel service
STORED MESSAGES for UE Channel service (service 0/peer 0)
STATE <Process messages> for UE Channel service
REQUESTED FOR REMOTE <Process messages> for UE Channel service
REQUESTED FROM REMOTE <Process messages> for UE Channel service

Priority UE Channel 0 service

TOTAL TRANSMITTED MESSAGES <2942> for UE Channel service
RECEIVED MESSAGES <11> for UE Channel service
SEND MESSAGES <2931> for UE Channel service
HALT REQUEST SEND COUNTER <0> for UE Channel service
STORED MESSAGES for UE Channel service (service 0/peer 0)
STATE <Process messages> for UE Channel service
REQUESTED FOR REMOTE <Process messages> for UE Channel service
REQUESTED FROM REMOTE <Process messages> for UE Channel service

TOTAL TRANSMITTED MESSAGES <29286> for FSTREAM service
RECEIVED MESSAGES <14648> for FSTREAM service
SEND MESSAGES <14638> for FSTREAM service


***********************
**RPC STATUS****10.83.57.41*************
'ip' => '10.83.57.41',
'uuid' => 'c03cb3c2-8fe2-11e6-bce8-8c278d49b0dd',
'ipv6' => '2001:420:2710:2556:1:0:0:41',
'name' => '10.83.57.41',
'active' => '1',
'uuid_gw' => '',
'last_changed' => 'Tue Oct 11 19:32:20 2016'

Check routes:

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure manager add</td>
<td>Adds a remote manager, Firepower Management Center.</td>
</tr>
</tbody>
</table>
show aaa-server

To display statistics for AAA servers, use the show **aaa-server** command.

```plaintext
show aaa-server  [ LOCAL |  groupname  [ host  hostname  |  protocol  protocol ]
```

### Syntax Description
- **groupname** *(Optional)* Show statistics for servers in a group.
- **host  hostname** *(Optional)* Show statistics for a particular server in the group.
- **LOCAL** *(Optional)* Show statistics for the LOCAL user database.
- **protocol  protocol** *(Optional)* Shows statistics for servers of the specified protocol: **ldap** or **radius**.

### Command Default
By default, all AAA server statistics display.

### Command History
- **Release**  **Modification**
  - 6.2.1  This command was introduced.

### Usage Guidelines
The following table shows field descriptions for the output of the **show aaa-server** command:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Group</td>
<td>The server group name.</td>
</tr>
<tr>
<td>Server Protocol</td>
<td>The server protocol for the server group.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The IP address of the AAA server.</td>
</tr>
<tr>
<td>Server port</td>
<td>The communication port used by the system and the AAA server.</td>
</tr>
<tr>
<td>Server status</td>
<td>The status of the server. If the status is followed by “(admin initiated),” then the server was manually failed or reactivated using the <strong>aaa-server active</strong> or <strong>aaa-server fail</strong> command. Values are:</td>
</tr>
<tr>
<td></td>
<td>• ACTIVE—The system will communicate with this AAA server.</td>
</tr>
<tr>
<td></td>
<td>• FAILED—The system cannot communicate with the AAA server. Servers that are put into this state remain there for some period of time, depending on the policy configured, and are then reactivated.</td>
</tr>
</tbody>
</table>

The date and time of the last transaction appears in one of the following form:

- **Last Transaction success at time timezone date**
- **Last Transaction failure at time timezone date**
- **Last Transaction at Unknown, if the device has not yet communicated with the server.**
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of pending requests</td>
<td>The number of requests that are still in progress.</td>
</tr>
<tr>
<td>Average round trip time</td>
<td>The average time that it takes to complete a transaction with the server.</td>
</tr>
<tr>
<td>Number of authentication requests</td>
<td>The number of authentication requests sent by the system. This value does not include retransmissions after a timeout.</td>
</tr>
<tr>
<td>Number of authorization requests</td>
<td>The number of authorization requests. This value refers to authorization requests due to command authorization, authorization for through-the-box traffic, or for WebVPN and IPsec authorization functionality enabled for a tunnel group. This value does not include retransmissions after a timeout.</td>
</tr>
<tr>
<td>Number of accounting requests</td>
<td>The number of accounting requests. This value does not include retransmissions after a timeout.</td>
</tr>
<tr>
<td>Number of retransmissions</td>
<td>The number of times a message was retransmitted after an internal timeout. This value applies only to RADIUS servers (UDP).</td>
</tr>
<tr>
<td>Number of accepts</td>
<td>The number of successful authentication requests.</td>
</tr>
<tr>
<td>Number of rejects</td>
<td>The number of rejected requests. This value includes error conditions as well as true credential rejections from the AAA server.</td>
</tr>
<tr>
<td>Number of challenges</td>
<td>The number of times the AAA server required additional information from the user after receiving the initial username and password information.</td>
</tr>
<tr>
<td>Number of malformed responses</td>
<td>This value is not meaningful.</td>
</tr>
<tr>
<td>Number of bad authenticators</td>
<td>This value only applies to RADIUS. The number of times that the “authenticator” string in the RADIUS packet is corrupted (rare), or the shared secret key on the system does not match the one on the RADIUS server. To fix this problem, enter the correct server key.</td>
</tr>
<tr>
<td>Number of timeouts</td>
<td>The number of times the system has detected that a AAA server is not responsive or otherwise misbehaving and has declared it offline.</td>
</tr>
<tr>
<td>Number of unrecognized responses</td>
<td>The number of times that the system received a response from the AAA server that it could not recognize or support. For example, the RADIUS packet code from the server was an unknown type, something other than the known “access-accept,” “access-reject,” “access-challenge,” or “accounting-response” types. Typically, this means that the RADIUS response packet from the server was corrupted, which is rare.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display the AAA statistics for a specific server in a group:

```
> show aaa-server group1 host 192.68.125.60
Server Group: group1
```
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC Fri Aug 22
Number of pending requests 20
Average round trip time 4ms
Number of authentication requests 20
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 1
Number of accepts 16
Number of rejects 4
Number of challenges 5
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 0
Number of unrecognized responses 0

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear aaa-server statistics</td>
<td>Clears AAA server statistics.</td>
</tr>
</tbody>
</table>
show access-control-config

To display summary information about your access control policy, use the `show access-control-config` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command provides a summary explanation of your Access Control Policy, including the characteristics of each access control rule. The output shows the name and description of the Access Control Policy, its default action, Security Intelligence policies, and information about the access control rule sets and each access control rule. It also shows the name of referenced SSL, network analysis, intrusion, and file policies; intrusion variable set data; logging settings; and other advanced settings, including policy-level performance, preprocessing, and general settings.

The information includes policy-related connection information, such as source and destination port data (including type and code for ICMP entries) and the number of connections that matched each access control rule (hit counts).

The information also shows the HTML used for the block and interactive block actions for URL filtering.

If you are using Firepower Device Manager (the local manager), unsupported features will either show their default settings or they will be empty. If you are using Firepower Management Center, you can adjust any of these settings using the manager. You cannot configure any of the rules or options shown in this output using the CLI; you must use the manager.

**Examples**

The following example shows the access control configuration for a device managed using Firepower Device Manager, the local manager.

```plaintext
> show access-control-config

==================[ NGFW-Access-Policy ]==================
Description : 

==================[ Default Action ]==================
Default Action : Block

Logging Configuration
  DC : Enabled
  Beginning : Disabled
  End : Disabled

Rule Hits : 0

Variable Set : Default-Set

---[ Security Intelligence - Network Whitelist ]---
---[ Security Intelligence - Network Blacklist ]---
Logging Configuration : Disabled
DC : Disabled

---[ Security Intelligence - URL Whitelist ]---
---[ Security Intelligence - URL Blacklist ]---
```
Logging Configuration : Disabled
DC : Disabled

----------[ Security Intelligence - DNS Policy ]----------
Name : Default DNS Policy

----------[ Rule Set: admin_category (Built-in) ]----------

----------[ Rule Set: standard_category (Built-in) ]----------

----------[ Rule: Inside_Inside_Rule ]----------
Action : Fast-path
Source Zones : inside_zone
Destination Zones : inside_zone
Users
URLs
Logging Configuration
DC : Enabled
Beginning : Enabled
End : Enabled
Files : Disabled
Safe Search : No
Rule Hits : 0
Variable Set : Default-Set

----------[ Rule: Inside_Outside_Rule ]----------
Action : Fast-path
Source Zones : inside_zone
Destination Zones : outside_zone
Users
URLs
Logging Configuration
DC : Enabled
Beginning : Enabled
End : Enabled
Files : Disabled
Safe Search : No
Rule Hits : 0
Variable Set : Default-Set

----------[ Rule: root_category (Built-in) ]----------

----------[ Advanced Settings ]----------
General Settings
Maximum URL Length : 1024
Interactive Block Bypass Timeout : 600
Do not retry URL cache miss lookup : No
Inspect Traffic During Apply : Yes
Network Analysis and Intrusion Policies
Initial Intrusion Policy : Balanced Security and Connectivity
Initial Variable Set : Default-Set
Default Network Analysis Policy : Balanced Security and Connectivity
Files and Malware Settings
File Type Inspect Limit : 1460
Cloud Lookup Timeout : 2
Minimum File Capture Size : 6144
Maximum File Capture Size : 1048576
Min Dynamic Analysis Size : 15360
Max Dynamic Analysis Size : 2097152
Malware Detection Limit : 10485760
Transport/Network Layer Preprocessor Settings
Detection Settings
Ignore VLAN Tracking Connections : No
Maximum Active Responses : No Maximum
Minimum Response Seconds : No Minimum
Session Termination Log Threshold : 1048576
Detection Enhancement Settings
Adaptive Profile : Disabled
Performance Settings
Event Queue
Maximum Queued Events : 5
Disable Reassembled Content Checks: False
Performance Statistics
Sample time (seconds) : 300
Minimum number of packets : 10000
Summary : False
Log Session/Protocol Distribution : False
Regular Expression Limits
Match Recursion Limit : Default
Match Limit : Default
Rule Processing Configuration
Logged Events : 5
Maximum Queued Events : 8
Events Ordered By : Content Length
Intelligent Application Bypass Settings
State : Off
Latency-Based Performance Settings
Packet Handling : Disabled

---

HTTP/1.1 403 Forbidden
Connection: close
Content-Length: 506
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<title>Access Denied</title>
<style>body {margin:0;font-family:verdana,sans-serif;}

h1 {margin:0;padding:12px 25px;background-color:#343434;color:#ddd}

p {margin:12px 25px;}

strong {color:#E0042D;}
</style>
</head>
<body>
<h1>Access Denied</h1>
<p><strong>You are attempting to access a forbidden site.</strong><br/>
Consult your system administrator for details.<br/>
</p>
</body>
</html>

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-list</td>
<td>Shows the contents of Access Control Lists (ACLs).</td>
</tr>
</tbody>
</table>
To display the rules and hit counters for an access list, use the `show access-list` command.

```
show access-list [ id [ ip_address | brief ] ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>id</code></td>
<td>(Optional) The name of an existing access list, to limit the view to this one access list.</td>
</tr>
<tr>
<td><code>ip_address</code></td>
<td>(Optional) The source IPv4 or IPv6 address, to limit the view to rules with this address.</td>
</tr>
<tr>
<td><code>brief</code></td>
<td>(Optional) Displays the access list identifiers, the hit count, and the time stamp of the last rule hit, all in hexadecimal format.</td>
</tr>
<tr>
<td><code>numeric</code></td>
<td>(Optional.) If you specify an ACL name, displays ports as numbers instead of names. For example, 80 instead of www.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The system structures some elements of the Access Control Policy as advanced access control list (ACL) entries. When possible, access control rules that block traffic based on layer 3 criteria become deny rules in the ACL. You might also see trust ACL rules that align with trust access control rules.

But if an access control rule requires inspection, even if the rule action is block, the ACL entry actually permits the traffic. This permitted traffic is then passed to the inspection engines, such as snort, which can ultimately block unwanted traffic.

Thus, there is not a one-to-one relationship between the low-level ACL rules shown with `show access-list` and the Access Control Policy rules for the device. The advanced ACL allows the system to make early drop or trust decisions on traffic, so connections that do not need inspection can be passed or dropped as quickly as possible.

ACLs can also be used for other things, such as route maps and match criteria for service policies. Standard and extended ACLs are used for these purposes.

You can display multiple access lists at one time by entering the access list identifiers in one command.

You can specify the `brief` keyword to display access list hit count, identifiers, and timestamp information in hexadecimal format. The configuration identifiers displayed in hexadecimal format are presented in three columns, and they are the same identifiers used in syslogs 106023 and 106100.

If an access list has been changed recently, the list is excluded from the output. A message will indicate when this happens.

**Note**

The output shows how many elements are in the ACL. This number is not necessarily the same as the number of access control entries (ACE) in the ACL. The system might create extra elements when you use network objects with address ranges, for example, and these extra elements are not included in the output.
Clustering Guidelines

When using clustering, if traffic is received by a single unit, the other units may still show a hit count for the ACL due to the clustering director logic. This is an expected behavior. Because the unit that did not receive any packets directly from the client may receive forwarded packets over the cluster control link for an owner request, the unit may check the ACL before sending the packet back to the receiving unit. As a result, the ACL hit count will be increased even though the unit did not pass the traffic.

Examples

The following is sample output from the `show access-list` command and shows the advanced access list generated for the Access Control Policy when using Firepower Device Manager (the local or “on box” manager). The remarks are system-generated to help you understand the access control entries (ACEs). Note that the remarks give you the name of the related rule; ACEs generated from the rule follow. These remarks are highlighted in the example below.

```plaintext
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list NGFW_ONBOX_ACL; 50 elements; name hash: 0xf5cc3f88
access-list NGFW_ONBOX_ACL line 1 remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 2 remark rule-id 268435458: L5 RULE: Inside_Inside_Rule
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any rule-id 268435458 event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any rule-id 268435458 event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any rule-id 268435458 event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any rule-id 268435458 event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any rule-id 268435458 event-log both (hitcnt=0) 0x05478586
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any rule-id 268435458 event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any rule-id 268435458 event-log both (hitcnt=0) 0xc1579ed7
access-list NGFW_ONBOX_ACL line 10 advanced trust ip ifc inside1_3 any ifc inside1_4 any rule-id 268435458 event-log both (hitcnt=0) 0x40968b8f
access-list NGFW_ONBOX_ACL line 11 advanced trust ip ifc inside1_3 any ifc inside1_5 any rule-id 268435458 event-log both (hitcnt=0) 0x8441043c
access-list NGFW_ONBOX_ACL line 12 advanced trust ip ifc inside1_3 any ifc inside1_6 any rule-id 268435458 event-log both (hitcnt=0) 0xd62c1560f
access-list NGFW_ONBOX_ACL line 13 advanced trust ip ifc inside1_3 any ifc inside1_7 any rule-id 268435458 event-log both (hitcnt=0) 0x35715335c
access-list NGFW_ONBOX_ACL line 14 advanced trust ip ifc inside1_3 any ifc inside1_8 any rule-id 268435458 event-log both (hitcnt=0) 0xc4a66c0a
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any rule-id 268435458 event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 16 advanced trust ip ifc inside1_4 any ifc inside1_3 any rule-id 268435458 event-log both (hitcnt=0) 0x8f7bbcdf
access-list NGFW_ONBOX_ACL line 17 advanced trust ip ifc inside1_4 any ifc inside1_5 any rule-id 268435458 event-log both (hitcnt=0) 0xe616991f
access-list NGFW_ONBOX_ACL line 18 advanced trust ip ifc inside1_4 any ifc inside1_6 any rule-id 268435458 event-log both (hitcnt=0) 0x4db9d2aa
access-list NGFW_ONBOX_ACL line 19 advanced trust ip ifc inside1_4 any ifc inside1_7 any rule-id 268435458 event-log both (hitcnt=0) 0xf8a88db4
access-list NGFW_ONBOX_ACL line 20 advanced trust ip ifc inside1_4 any ifc inside1_8 any rule-id 268435458 event-log both (hitcnt=0) 0x1d3b5b80
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
```

Cisco Firepower Threat Defense Command Reference
rule-id 268435458 event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 22 advanced trust ip ifc inside1_5 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x7084f3fc
access-list NGFW_ONBOX_ACL line 23 advanced trust ip ifc inside1_5 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xd989f9aa
access-list NGFW_ONBOX_ACL line 24 advanced trust ip ifc inside1_5 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xd5aa77f5
access-list NGFW_ONBOX_ACL line 25 advanced trust ip ifc inside1_5 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4a7648b2
access-list NGFW_ONBOX_ACL line 26 advanced trust ip ifc inside1_5 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_5 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0xda17cb9e
access-list NGFW_ONBOX_ACL line 29 advanced trust ip ifc inside1_6 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0x36203c1e
access-list NGFW_ONBOX_ACL line 30 advanced trust ip ifc inside1_6 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x05f085c3
access-list NGFW_ONBOX_ACL line 31 advanced trust ip ifc inside1_6 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4574192b
access-list NGFW_ONBOX_ACL line 32 advanced trust ip ifc inside1_6 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x36a1e6a1
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0x0x415bb76
access-list NGFW_ONBOX_ACL line 34 advanced trust ip ifc inside1_7 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x18ebff70
access-list NGFW_ONBOX_ACL line 35 advanced trust ip ifc inside1_7 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xf99725ea
access-list NGFW_ONBOX_ACL line 36 advanced trust ip ifc inside1_7 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x6e13508f
access-list NGFW_ONBOX_ACL line 37 advanced trust ip ifc inside1_7 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0x39b9fd690
access-list NGFW_ONBOX_ACL line 38 advanced trust ip ifc inside1_7 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x0x08a88b4
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0x2cfd43cd
access-list NGFW_ONBOX_ACL line 40 advanced trust ip ifc inside1_8 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x39c65e52
access-list NGFW_ONBOX_ACL line 41 advanced trust ip ifc inside1_8 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0x83c65e52
The following examples show brief information about the specified access policy in hexadecimal format (ACEs in which the hitcount is not zero). The first two columns display identifiers in hexadecimal format, the third column lists the hit count, and the fourth column displays the timestamp value, also in hexadecimal format. The hit count value represents the number of times the rule has been hit by traffic. The timestamp value reports the time of the last hit. If the hit count is zero, no information is displayed.

The following is sample output from the `show access-list brief` command when Telnet traffic is passed:

```
> show access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
```

The following is sample output from the `show access-list brief` command when SSH traffic is passed:

```
> show access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922 44ae5901 00000001 4a68ab66
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear access-list</td>
<td>Clears an access list counter.</td>
</tr>
<tr>
<td>show running-config access-list</td>
<td>Displays the current running access-list configuration.</td>
</tr>
</tbody>
</table>
show alarm settings

To display the configuration for each type of alarm in the ISA 3000, use the `show alarm settings` command.

```
> show alarm settings

Power Supply
  Alarm: Disabled
  Relay: Disabled
  Notifies: Disabled
  Syslog: Disabled

Temperature-Primary
  Alarm: Enabled
  Thresholds: MAX: 92C, MIN: -40C
  Relay: Enabled
  Notifies: Enabled
  Syslog: Enabled

Temperature-Secondary
  Alarm: Disabled
  Threshold: Disabled
  Relay: Disabled
  Notifies: Disabled
  Syslog: Disabled

Input-Alarm 1
  Alarm: Enabled
  Relay: Disabled
  Notifies: Disabled
  Syslog: Enabled

Input-Alarm 2
  Alarm: Enabled
  Relay: Disabled
  Notifies: Disabled
  Syslog: Enabled
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is a sample output from the `show alarm settings` command:

```
> show alarm settings

Power Supply
  Alarm: Disabled
  Relay: Disabled
  Notifies: Disabled
  Syslog: Disabled

Temperature-Primary
  Alarm: Enabled
  Thresholds: MAX: 92C, MIN: -40C
  Relay: Enabled
  Notifies: Enabled
  Syslog: Enabled

Temperature-Secondary
  Alarm: Disabled
  Threshold: Disabled
  Relay: Disabled
  Notifies: Disabled
  Syslog: Disabled

Input-Alarm 1
  Alarm: Enabled
  Relay: Disabled
  Notifies: Disabled
  Syslog: Enabled

Input-Alarm 2
  Alarm: Enabled
  Relay: Disabled
  Notifies: Disabled
  Syslog: Enabled
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear facility-alarm output</td>
<td>De-energizes the output relay and clears the alarm state of the LED.</td>
</tr>
<tr>
<td>show environment alarm-contact</td>
<td>Displays the status of the input alarm contacts.</td>
</tr>
<tr>
<td>show facility-alarm</td>
<td>Displays status information for triggered alarms.</td>
</tr>
</tbody>
</table>
show app-agent heartbeat

To display the status of the app-agent, use the `show app-agent heartbeat` command.

```
show app-agent heartbeat
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The app-agent heartbeat communication channel serves the purpose of monitoring the health of the link between FXOS chassis supervisor and Firepower Threat Defense application agent. This is used if you configure hardware bypass on Firepower 4100 or 9300 series devices. It is not used with other device models running Firepower Threat Defense software.

Use the `show app-agent heartbeat` command to view status on the app-agent heartbeat communication channel.

**Examples**

The following example shows the app-agent heartbeat status.

```
> show app-agent heartbeat
appagent heartbeat timer 1 retry-count 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>app-agent</td>
<td>Configures the app-agent for Hardware Bypass.</td>
</tr>
</tbody>
</table>
show arp

To view the ARP table, use the `show arp` command.

```
show arp
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The display output shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds. Static ARP entries include a dash (-) instead of the age, and proxy ARP entries state “alias.”

The ARP table can include entries for internal interfaces, such as `nlp_int_tap`, which are used for system communications.

### Examples

The following is sample output from the `show arp` command. The first entry is a dynamic entry aged 2 seconds. The second entry is a static entry, and the third entry is from proxy ARP.

```
> show arp
outside 10.86.194.61 0011.2094.1d2b 2
outside 10.86.194.1 001a.300c.8000 -
outside 10.86.195.2 00d0.02a8.440a alias
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear arp statistics</td>
<td>Clears ARP statistics.</td>
</tr>
<tr>
<td>show arp statistics</td>
<td>Shows ARP statistics.</td>
</tr>
<tr>
<td>show running-config all arp</td>
<td>Shows the current configuration of the ARP timeout.</td>
</tr>
</tbody>
</table>
show arp-inspection

To view the ARP inspection setting for each interface, use the `show arp-inspection` command.

```
show arp-inspection
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was added.</td>
</tr>
<tr>
<td>6.2</td>
<td>Support for routed mode was added.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show arp-inspection` command:

```
> show arp-inspection
interface                      arp-inspection     miss
inside1                        enabled              flood
outside                        disabled             -
```

The miss column shows the default action to take for non-matching packets when ARP inspection is enabled, either “flood” or “no-flood.”

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear arp statistics</td>
<td>Clears ARP statistics.</td>
</tr>
<tr>
<td>show arp statistics</td>
<td>Shows ARP statistics.</td>
</tr>
<tr>
<td>show running-config all arp</td>
<td>Shows the current configuration of the ARP timeout.</td>
</tr>
</tbody>
</table>
show arp statistics

To view ARP statistics, use the `show arp statistics` command.

```
show arp statistics
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show arp statistics` command:

```
> show arp statistics
  Number of ARP entries:
  ASA : 6
  Dropped blocks in ARP: 6
  Maximum Queued blocks: 3
  Queued blocks: 1
  Interface collision ARPs Received: 5
  ARP-defense Gratuitous ARPS sent: 4
  Total ARP retries: 15
  Unresolved hosts: 1
  Maximum Unresolved hosts: 2
```

The following table explains each field.

*Table 2: show arp statistics Fields (continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of ARP entries</td>
<td>The total number of ARP table entries.</td>
</tr>
<tr>
<td>Dropped blocks in ARP</td>
<td>The number of blocks that were dropped while IP addresses were being resolved to their corresponding hardware addresses.</td>
</tr>
<tr>
<td>Maximum queued blocks</td>
<td>The maximum number of blocks that were ever queued in the ARP module, while waiting for the IP address to be resolved.</td>
</tr>
<tr>
<td>Queued blocks</td>
<td>The number of blocks currently queued in the ARP module.</td>
</tr>
<tr>
<td>Interface collision ARPs received</td>
<td>The number of ARP packets received at all interfaces that were from the same IP address as that of an interface.</td>
</tr>
<tr>
<td>ARP-defense gratuitous ARPS sent</td>
<td>The number of gratuitous ARPs sent by the device as part of the ARP-Defense mechanism.</td>
</tr>
<tr>
<td>Total ARP retries</td>
<td>The total number of ARP requests sent by the ARP module when the address was not resolved in response to first ARP request.</td>
</tr>
</tbody>
</table>
The number of unresolved hosts for which ARP requests are still being sent out by the ARP module.

The maximum number of unresolved hosts that ever were in the ARP module since it was last cleared or the device booted up.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unresolved hosts</td>
<td>The number of unresolved hosts for which ARP requests are still being sent out by the ARP module.</td>
</tr>
<tr>
<td>Maximum unresolved hosts</td>
<td>The maximum number of unresolved hosts that ever were in the ARP module since it was last cleared or the device booted up.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear arp statistics</td>
<td>Clears ARP statistics.</td>
</tr>
<tr>
<td>show arp</td>
<td>Shows the ARP table.</td>
</tr>
<tr>
<td>show running-config all arp</td>
<td>Shows the current configuration of the ARP timeout.</td>
</tr>
</tbody>
</table>
show as-path-access-list

To display the contents of all current autonomous system (AS) path access lists, use the show as-path-access-list command.

**Syntax Description**

```
show as-path-access-list [number]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>(Optional) Specifies the AS path access list number. Valid values are between 1 and 500.</td>
</tr>
</tbody>
</table>

**Command Default**

If the `number` argument is not specified, command output is displayed for all AS path access lists.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show as-path-access-list` command:

```
> show as-path-access-list
AS path access list 1
AS path access list 2
```
show asp cluster counter

To debug global or context-specific information in a clustering environment, use the `show asp cluster counter` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show asp cluster counter` command shows the global and context-specific DP counters, which might help you troubleshoot a problem. This information is used for debugging purposes only, and the information output is subject to change. Consult the Cisco TAC to help you debug your system with this command.

**Examples**

The following is sample output from the `show asp cluster counter` command:

```
> show asp cluster counter
Global dp-counters:
Context specific dp-counters:
  MCAST_FP_TO_SP 361136
  MCAST_SP_TOTAL 361136
  MCAST_SP_PKTS 143327
  MCAST_SP_PKTS_TO_CP 143327
  MCAST_FP_CHK_FAIL_NO_HANDLE 217809
  MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC 81192
  MCAST_FP_CHK_FAIL_NO_FP_FWD 62135
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show asp drop</td>
<td>Shows the accelerated security path counters for dropped packets.</td>
</tr>
</tbody>
</table>
show asp dispatch

To display statistics for the device’s load balance ASP dispatcher, which is useful for diagnosing performance issues, use the `show asp dispatch` command. It is only available for a Firepower Threat Defense virtual device in the hybrid poll/interrupt mode.

**show asp dispatch**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show asp dispatch` command.

```
> show asp dispatch
---- Lina DP thread dispatch stats - CORE 0 ----
Dispatch loop count : 92260212
Dispatch C2C poll count : 2
CP scheduler busy : 14936242
CP scheduler idle : 77323971
RX ring busy : 1513632
Async lock global q busy : 809481
Global timer q busy : 1958684
SNP flow bulk sync busy : 174
Purg process busy : 2838
Block attempts : 44594355
Maximum timeout specified : 10000000
Minimum timeout specified : 1572864
Average timeout specified : 9999994
Waken up with OK status : 2476791
Waken up with timeout : 42117564
Sleep interrupted : 85753
Number of interrupts : 2492566
Number of RX interrupts : 1454442
Number of TX interrupts : 2492566
Enable interrupt ok : 174566236
Disable interrupt ok : 174231423
Maximum elapsed time : 54082257
Minimum elapsed time : 6165
Average elapsed time : 9658532
Message pipe stats :  

Last clearing of asp dispatch: Never

---- Lina DP thread home-ring/interface list - CORE 0 ----
Interface Internal-Data0/0: port-id 0 irq 10 fd 37
Interface GigabitEthernet0/0: port-id 256 irq 5 fd 38
Interface GigabitEthernet0/1: port-id 512 irq 9 fd 39
Interface GigabitEthernet0/2: port-id 768 irq 11 fd 40
> 
```
show asp drop

To debug the accelerated security path dropped packets or connections, use the `show asp drop` command.

```
show asp drop [flow [flow_drop_reason] | frame [frame_drop_reason]]
```

**Syntax Description**

- **flow [flow_drop_reason]** (Optional) Shows the dropped flows (connections). You can optionally specify a particular reason. Use `?` to see a list of possible flow drop reasons.

- **frame [frame_drop_reason]** (Optional) Shows the dropped packets. You can optionally specify a particular reason. Use `?` to see a list of possible frame drop reasons.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show asp drop` command shows the packets or connections dropped by the accelerated security path, which might help you troubleshoot a problem. This information is used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.


**Examples**

The following is sample output from the `show asp drop` command, with the time stamp indicating the last time the counters were cleared:

```
> show asp drop

Frame drop:
Flow is denied by configured rule (acl-drop) 3
Dst MAC L2 Lookup Failed (dst-l2_lookup-fail) 4110
L2 Src/Dst same LAN port (l2_same-lan-port) 760
Expired flow (flow-expired) 1

Last clearing: Never

Flow drop:
Flow is denied by access rule (acl-drop) 24
NAT failed (nat-failed) 28739
NAT reverse path failed (nat-rpf-failed) 22266
Inspection failure (inspect-fail) 19433

Last clearing: 17:02:12 UTC Jan 17 2012 by enable_15
```
show asp event

To debug the data path or control path event queues, use the show asp event command.

show asp event {dp-cp | cp-dp}

Syntax Description

| dp-cp | Show events sent from the ASP data-path to the control plane. |
| cp-dp | Show events sent from the control plane to the ASP data-path. |

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The show asp event command shows the contents of the data path and control path, which might help you troubleshoot a problem. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the show asp event dp-cp command:

```
> show asp event dp-cp
DP-CP EVENT QUEUE QUEUE-LEN HIGH-WATER
Punt Event Queue 0 0
Routing Event Queue 0 0
Identity-Traffic Event Queue 0 1
PTP-Traffic Event Queue 0 0
General Event Queue 0 0
Syslog Event Queue 0 0
Non-Blocking Event Queue 0 8
Midpath High Event Queue 0 0
Midpath Norm Event Queue 0 0
Crypto Event Queue 0 146
HA Event Queue 0 0
Threat-Detection Event Queue 0 0
SCP Event Queue 0 0
ARP Event Queue 0 1
IDFW Event Queue 0 0
CXSC Event Queue 0 0
BFD Event Queue 0 0

EVENT-TYPE ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL RETIRED 15SEC-RATE
crypto-msg 810 0 810 0 810 0
arp-in 17288 0 17288 0 17288 0
identity-traffic 2 0 2 0 2 0
scheduler 239 0 239 0 239 0
```
show asp inspect-dp egress-optimization

Displays statistics about egress optimization, a feature that enhances performance. Use this command on the advice of Cisco TAC.

show asp inspect-dp egress-optimization

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The show asp inspect-dp egress-optimization command displays information about flows eligible for egress optimization, a feature that enhances performance. The output displays the following information:

- Current running state: Whether egress optimization is enabled or disabled.
- Flow (a flow consists of one or more packets):
  - Current: Number of flows that are currently eligible for egress optimization processing.
  - Maximum: Total number of egress-optimization eligible flows since the last time inspection engine was restarted or egress optimization statistics were cleared.
- Packet:
  - Processed: Total number of packets processed.
  - Expected: Number of packets that were initially determined to be eligible for egress optimization but later determined to be ineligible for egress optimization.

Examples

The following is sample output from the show asp inspect-dp egress-optimization command.

```plaintext
> show asp inspect-dp egress-optimization
Current running state: Enabled
Flow:
  current: 1, maximum: 3
  snort-unreachable: 0, snort-unsupported-header: 1, snort-unsupported-verdict: 2
Packet:
  processed: 5
  excepted: 0
```

Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear asp inspect-dp egress-optimization</td>
<td>Clears egress optimization statistics.</td>
</tr>
<tr>
<td>Commands</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show asp inspect-dp egress-optimization</td>
<td>Displays information about flows eligible for egress optimization. Use this command on the advice of Cisco TAC.</td>
</tr>
</tbody>
</table>
show asp inspect-dp snapshot

To view the snapshot of a PDTS (data plane transmit/receive queues to snort) ring, use the show asp inspect-dp snapshot command.

`show asp inspect-dp snapshot { config | instance instance_id queue queue_id }`

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Displays the global configuration for PDTS snapshots.</td>
</tr>
<tr>
<td>instance instance_id</td>
<td>Displays snapshot for the specified PDTS consumer instance ID. Values are from 0-2147483647.</td>
</tr>
<tr>
<td>queue queue_id</td>
<td>Displays the snapshot for the specified data path transmit queue ID of a PDTS ring. Values are from 0-2147483647.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show asp inspect-dp snapshot` command displays the global configurations of the PDTS ring snapshot feature. The output displays the following information:

- Max snapshots: The maximum number of auto snapshots allowed.
- Current in use: The number of snapshots that have been stored so far.
- Interval: The time interval value specifies how long two snapshots on the same PDTS ring are allowed
- Auto Snapshot: Show if auto PDTS snapshot feature is enabled or disabled

**Examples**

The following is sample output from the `show asp inspect-dp snapshot config` command.

```
> show asp inspect-dp snapshot config
Max snapshots | Current in use | Interval (min) | Auto Snapshot
---------------|---------------|----------------|----------------|
2              | 0             | 5              | OFF            |
```

The following is sample output from the `show asp inspect-dp snapshot instance` command.

```
> show asp inspect-dp snapshot instance 2 queue 1
0 packet captured
0 packet shown
```
show asp inspect-dp snort

To display the status of all snort instances, use the `show asp inspect-dp snort` command.

```
show asp inspect-dp snort [instance  instance_id]
```

### Syntax Description

| instance instance_id | Displays the status of the specific snort instance. Values for instance_id are from 0-2147483647. |

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays the status of all snort instances. The output displays the following information:

- **Id**: SNORT instance ID.
- **PID**: Snort instance process ID.
- **CPU-Usage**: CPU usage for the snort instance ID. Printed in total, and user/sys. **Note**: This field is not shown for the Firepower 2100 series.
- **Conns**: Number of connections currently held by the snort instance.
- **Segs/Pkts**: Number of segments or say packets currently processed by the snort instance.
- **Status**: The status of the snort instance.

### Examples

The following is sample output from the `show asp inspect-dp snort` command.

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

<table>
<thead>
<tr>
<th>Id</th>
<th>Pid</th>
<th>Cpu-Usage</th>
<th>Conns</th>
<th>Segs/Pkts</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>9188</td>
<td>0% ( 0%</td>
<td>0%) 0</td>
<td>0</td>
<td>READY</td>
</tr>
<tr>
<td>1</td>
<td>9187</td>
<td>0% ( 0%</td>
<td>0%) 0</td>
<td>0</td>
<td>READY</td>
</tr>
<tr>
<td>2</td>
<td>9186</td>
<td>0% ( 0%</td>
<td>0%) 0</td>
<td>0</td>
<td>READY</td>
</tr>
</tbody>
</table>
```

The following is sample output from the `show asp inspect-dp snort` command on the Firepower 2100.

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

<table>
<thead>
<tr>
<th>Id</th>
<th>Pid</th>
<th>Conns</th>
<th>Segs/Pkts</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>30080</td>
<td>40</td>
<td>0</td>
<td>READY</td>
</tr>
<tr>
<td>1</td>
<td>30081</td>
<td>14</td>
<td>0</td>
<td>READY</td>
</tr>
<tr>
<td>2</td>
<td>30079</td>
<td>20</td>
<td>0</td>
<td>READY</td>
</tr>
</tbody>
</table>
show asp inspect-dp snort counters

To display the PDTS related raw counters for snort instances, use the `show asp inspect-dp snort counters` command.

show asp inspect-dp snort counters [instance  instance_id] [queues] [rate] [debug] [zeros]

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance</td>
<td>Displays the counters for the specific snort instance. Values are from 0-2147483647.</td>
</tr>
<tr>
<td>queues</td>
<td>Displays the queues information in detail. Each producer queue for the instance is displayed separately. Queue information of an instance will not be aggregated.</td>
</tr>
<tr>
<td>rate</td>
<td>It takes the counters snapshot for 5 seconds, averaged to one sec, and shows the rate of the counter changes.</td>
</tr>
<tr>
<td>debug</td>
<td>It displays certain debug counters not otherwise displayed.</td>
</tr>
<tr>
<td>zeros</td>
<td>All counters including zero counters will be displayed.</td>
</tr>
</tbody>
</table>

**Command Default**

If no instance is specified, all instances are displayed.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the PDTS related raw counters for snort instances. The output displays the following information:

- **Id**: Snort instance ID. “All” means all snort instances aggregated.
- **QId**: Lina transmit queue ID. It corresponds to the number of Lina threads. “All” means all the queues are aggregated.
- **Type**: Type of the counter. Data counter, error counter, debug counters, etc.
- **Name**: Name of the counter.
- **Value**: Human readable value of the counter.
- **Raw-Value**: Raw value of the counter.

**Counter Names**:

- **Tx Bytes**: Number of bytes Lina sent to the snort instance.
- **Tx Segs**: Number of frames/segments Lina sent to the snort instance.
- **Rx Bytes**: Number of bytes Lina received from the snort instance.
- **Rx Segs**: Number of frames/segments Lina received from the snort instance.
- **NewConns**: Number of connections sent to the snort instance.
• RxQ-Wakeup
• TxQ-Wakeup
• TxQ-LB-Dynamic: Number of times the PDTS dynamic load balancing kicked in.
• TxQ-Data-Hi-Thresh: Number of times the High threshold limit on Lina’s transmit queue is hit.
• RxQ-Full: Number of times the Lina’s receive queue gets full.
• TxQ-Full: Number of times the Lina’s transmit queue gets full.
• TxQ-Data-Limit: Number of times the data limit on Lina’s transmit queue is hit.
• TxQ-LB-Failed: Number of times the PDTS dynamic load balancing failed.
• TxQ-Unavail: Number of times Lina’s transmit queue is unavailable.
• TxQ-Not-Ready: Number of times Lina’s transmit queue is not ready.
• TxQ-Suspended: Number of times Lina’s transmit queue is suspended.
• RxQ-Unavail: Number of times Lina’s receive queue is unavailable.
• RxQ-Not-Ready: Number of times Lina’s receive queue is not ready.
• RxQ-Suspended: Number of times Lina’s receive queue is suspended.

Examples
The following is sample output from the `show asp inspect-dp snort counters` command.

```
> show asp inspect-dp snort counters summary instance 5 debug zeros
SNORT Inspect Instance Counters
Id QId Type Name Value Raw-Value
-- ---- ---- ---- --------- ----------
5 All data Tx Bytes 3.3 GB (3549197468)
5 All data Tx Segs 4.7 M (4671722)
5 All data Rx Bytes 3.3 GB (3495936190)
5 All data Rx Segs 4.7 M (4677344)
5 All data NewConnns 11.1 K (11103)
5 All debug RxQ-Wakeup 0 (0)
5 All debug TxQ-Wakeup 4.7 M (4655982)
5 All warn TxQ-LB-Dynamic 0 (0)
5 All warn TxQ-Data-Hi-Thresh 0 (0)
5 All drop RxQ-Full 0 (0)
5 All drop TxQ-Full 0 (0)
5 All drop TxQ-Data-Limit 0 (0)
5 All drop TxQ-Data-Limit 0 (0)
5 All err TxQ-Unavail 0 (0)
5 All err TxQ-Not-Ready 0 (0)
5 All err TxQ-Suspended 0 (0)
5 All err RxQ-Unavail 0 (0)
5 All err RxQ-Not-Ready 0 (0)
5 All err RxQ-Suspended 0 (0)
```
show asp inspect-dp snort counters summary

To display the PDTS related counters for snort instances, use the `show asp inspect-dp snort counters summary` command. Counters are aggregated to each instance.

```
show asp inspect-dp snort counters summary [instance  instance_id] [queues] [rate]
```

**Syntax Description**

- `instance instance_id` Displays the counters for the specific snort instance. Values are from 0-2147483647.
- `queues` Displays the queues information in detail. Each producer queue for the instance is displayed separately. Queue information of an instance will not be aggregated.
- `rate` Displays the one second average increase in the counter. Currently the one sec average is based on the delta increase between the last and current invocation of the command. This will change such that the delta increase is based on a 5 second rolling average, sampled once a second.

**Command Default**

If no instance is specified, all instances are displayed.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the PDTS related counters for snort instances. The output displays the following information:

- **Id**: Snort instance ID. “All” means all snort instances aggregated.
- **QId**: Lina transmit queue ID. It corresponds to the number of Lina threads.“All” means all the queues are aggregated.
- **TxBytes**: Total number of bytes Lina sent to the snort instance.
- **TxFrames**: Total number of frames/segments Lina sent to the snort instance.
- **RxBytes**: Total number of bytes Lina received from the snort instance.
- **RxFrames**: Total number of frames/segments Lina received from the snort instance.
- **Conns**: Total number of connections handled by the snort instance.

**Examples**

The following is sample output from the `show asp inspect-dp snort counters summary` command.

```
> show asp inspect-dp snort counters summary instance 2
SNORT Inspect Instance Counter Summary
Id  QId  TxBytes  TxFrames  RxBytes  RxFrames  Conns
--  ----  ----------  ----------  --------  --------  ------
2   All   0         0         0         0         0
```
show asp inspect-dp snort queues

To display the queue information for all snort instances (processes) aggregating all queues to the same instance, use the show asp inspect-dp snort queues command.

show asp inspect-dp snort queues [instance instance_id] [detail] [debug]

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance</td>
<td>Displays the queues for the specific snort instance. Values are from 0-2147483647.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays the queues information in detail. Each producer queue for the instance is displayed separately. Queue information of an instance will not be aggregated.</td>
</tr>
<tr>
<td>debug</td>
<td>Extra debug information will also be displayed.</td>
</tr>
</tbody>
</table>

**Command Default**

If no instance is specified, all instances are displayed.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the queue information for all snort instances (processes) aggregating all queue to the same instance. The output displays the following information:

- **Id**: Snort instance ID. “All” means all snort instances aggregated.
- **QId**: Lina transmit queue ID. It corresponds to the number of Lina threads.“All” means all the queues are aggregated.
- **Rx Queue**: Lina’s receive queue. “Used” shows amount of data, “util” is the queue utilization rate, and “state” shows the shared memory state.
- **TxQ**: Lina’s transmit queue. “Used” shows amount of data, “util” is the queueutilization rate, and “state” shows the shared memory state.

Counters:

- **RxQ-Size**: Lina’s receive queue size.
- **TxQ-Size**: Lina’s transmit queue size.
- **TxQ-Data-Limit**: The data limit of transmit queue. Once beyond this threshold, data packets will be dropped. The percentage shows the threshold value on the transmit queue.
- **TxQ-Data-Hi-Thresh**: The High threshold of transmit queue. Once beyond this threshold, PDTS dynamic load balancing will kick in to try balancing the flows to other snort instances.

**Examples**

The following is sample output from the show asp inspect-dp snort queues command.

> show asp inspect-dp snort counters summary instance 2
SNORT Inspect Instance Queue Configuration

RxQ-Size: 1 MB
TxQ-Size: 128 KB
TxQ-Data-Limit: 102.4 KB (80%)
TxQ-Data-Hi-Thresh: 35.8 KB (28%)

<table>
<thead>
<tr>
<th>Id</th>
<th>QId</th>
<th>RxQ (used)</th>
<th>RxQ (util)</th>
<th>TxQ (used)</th>
<th>TxQ (util)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>All</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>1</td>
<td>All</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>2</td>
<td>All</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>
show asp inspect-dp snort queue-exhaustion

To display the automatic snapshots of when a snort queue exhaustion occurs, use the `show asp inspect-dp snort queue-exhaustion` command.

```
show asp inspect-dp snort queue-exhaustion [snapshot snapshot_id] [export location]
```

**Syntax Description**

- **snapshot snapshot_id**  
  This option specifies a particular snapshot to print the queue exhaustion information. Values are between 1 and 24.

- **export location**  
  The contents of a snapshot are exported into a pcap file at the specified location, for off-box analysis.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show asp inspect-dp snort queue-exhaustion` command displays the contents of the snapshots taken when snort queues are exhausted. It shows the contents of a selected snapshot. The output is similar to the output of `show capture` command.

**Examples**

The following is sample output from the `show asp inspect-dp snort queue-exhaustion` command.

```
> show asp inspect-dp snort queue-exhaustion snapshot 1
102 packets captured
  693143043:693144411(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977907>
  693144411:693145779(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977907>
  693145779:693147147(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977912>
  693147147:693148515(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977912>
  693153987:693155355(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977932>
  (...output truncated...)  
```
show asp load-balance

To display a histogram of the load balancer queue sizes, use the `show asp load-balance` command.

```
show asp load-balance [detail]
```

**Syntax Description**

- `detail` (Optional) Shows detailed information about hash buckets used in the samples.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show asp load-balance` command might help you troubleshoot a problem. Normally a packet will be processed by the same core that pulled it in from the interface receive ring. However, if another core is already processing the same connection as the packet just received, then the packet will be queued to that core. This queuing can cause the load balancer queue to grow while other cores are idle. See the `asp load-balance per-packet` command for more information.

**Examples**

The following is sample output from the `show asp load-balance` command. The X-axis represents the number of packets queued in different queues. The Y-axis represents the number of load balancer hash buckets (not to be confused with the bucket in the histogram title, which refers to the histogram bucket) that has packets queued. To know the exact number of hash buckets having the queue, use the `detail` keyword.

```
> show asp load-balance
Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
  ASP load balancer queue sizes
  
100 +
  |
  |
S a m p l e s
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
  |
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>asp load-balance</code></td>
<td>Changes the core load balancing method for multi-core ASA models.</td>
</tr>
<tr>
<td><code>per-packet</code></td>
<td></td>
</tr>
</tbody>
</table>

show asp load-balance
**show asp multiprocessor accelerated-features**

To debug the accelerated security path multiprocessor accelerate, use the `show asp multiprocessor accelerated-features` command.

```plaintext
show asp multiprocessor accelerated-features
```

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show asp multiprocessor accelerated-features` command shows the lists of features accelerated for multiprocessors, which might help you troubleshoot a performance problem.

**Examples**

The following is sample output from the `show asp multiprocessor accelerated-features` command:

```plaintext
> show asp multiprocessor accelerated-features
MultiProcessor accelerated feature list:
  Access Lists
  DNS Guard
  Failover Stateful Updates
  Flow Operations(create, update, and tear-down)
  Inspect HTTP URL Logging
  Inspect HTTP (AIC)
  Inspect IPSec Pass through
  Inspect ICMP and ICMP error
  Inspect RTP/RTCP
  IP Audit
  IP Fragmentation & Re-assembly
  IPSec data-path
  MPF L2-L4 Classify
  Multicast forwarding
  NAT/PAT
  Netflow using UDP transport
  Non-AIC Inspect DNS
  Packet Capture
  QoS
  Resource Management
  Routing Lookup
  Shun
  SSL data-path
  Syslogging using UDP transport
  TCP Intercept
  TCP Security Engine
  TCP Transport
  Threat Detection
  Unicast RPF
  WCCP Re-direct
Above list applies to routed, transparent, single and multi mode.
```
show asp overhead

To track and display spin lock and async loss statistics, use the **show asp overhead** command.

`show asp overhead [sort-by-average] [sort-by-file]`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sort-by-average</td>
<td>Sorts the results by average cycles per call</td>
</tr>
<tr>
<td>sort-by-file</td>
<td>Sorts the results by filename</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the **show asp overhead** command:

```
> show asp overhead
0.0% of available CPU cycles were lost to Multiprocessor overhead
since last the MP overhead statistics were last cleared

File Name Line Function Call Avg Cycles %
---------------------------------------- ---- ---------------------- ----- ------------- ----
```
**show asp packet-profile**

To display the counters for how many packets were fastpathed by a prefilter policy, offloaded as a large flow, and fully evaluated by access control (Snort), use the `show asp packet-profile` command.

```plaintext
show asp packet-profile [data-path  offload  snort]
```

### Syntax Description

- **data-path**
  - Displays the counters for the data plane packet profiles.
- **offload**
  - Displays the counters for the hardware offload packet profiles.
- **snort**
  - Displays the counters for the snort packet profiles.

### Command Default

If no instance is specified, all instances are displayed.

### Command History

**Release** | **Modification**
--- | ---
6.5 | This command was introduced.

### Usage Guidelines

Each packet traversing a Firepower Threat Defense device goes through various stages of processing depending on the access policies configured, the Snort verdicts, and hardware capabilities like flow offload support.

Global counters are used to track these statistics and are updated at the end of each session. These global counters are collected and represented in the form of a histogram. At any given point the histogram displays the cumulative packet counters processed by the system since device boot up time or the last restart.

### Examples

The following is sample output from the `show asp packet-profile` command.

```plaintext
> show asp packet-profile
Current config state: Enabled
Packets Processed

-----------------------------
  hw-dynamic-offload : 0
  hw-static-offload : 0
  data-path-trust : 1419636
  data-path-snort : 3522634
  data-path-snort-bypass-allowedlist : 144496
  data-path-snort-bypass-blockedlist : 0
  data-path-snort-busy-failopen : 0
  data-path-snort-down-failopen : 10
-----------------------------
  data-path-snort-pre-allowedlist-distribution
Packets : Connections
[0-3] : 0
(4-7] : 6202
[8-15] : 10950
[16-31] : 2487
```
### data-path-snort-pre-blockedlist-distribution

<table>
<thead>
<tr>
<th>Packets</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0-3]</td>
<td>0</td>
</tr>
<tr>
<td>[4-7]</td>
<td>0</td>
</tr>
<tr>
<td>[8-15]</td>
<td>0</td>
</tr>
<tr>
<td>[16-31]</td>
<td>0</td>
</tr>
<tr>
<td>[32-63]</td>
<td>0</td>
</tr>
<tr>
<td>[64-127]</td>
<td>0</td>
</tr>
<tr>
<td>[128-255]</td>
<td>0</td>
</tr>
<tr>
<td>[256-511]</td>
<td>0</td>
</tr>
<tr>
<td>[512-1023]</td>
<td>0</td>
</tr>
<tr>
<td>[1024 and above]</td>
<td>0</td>
</tr>
</tbody>
</table>

### data-path-snort-post-allowedlist-distribution

<table>
<thead>
<tr>
<th>Packets</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0-3]</td>
<td>0</td>
</tr>
<tr>
<td>[4-7]</td>
<td>0</td>
</tr>
<tr>
<td>[8-15]</td>
<td>0</td>
</tr>
<tr>
<td>[16-31]</td>
<td>0</td>
</tr>
<tr>
<td>[32-63]</td>
<td>0</td>
</tr>
<tr>
<td>[64-127]</td>
<td>0</td>
</tr>
<tr>
<td>[128-255]</td>
<td>0</td>
</tr>
<tr>
<td>[256-511]</td>
<td>0</td>
</tr>
<tr>
<td>[512-1023]</td>
<td>0</td>
</tr>
<tr>
<td>[1024 and above]</td>
<td>0</td>
</tr>
</tbody>
</table>

### offload-post-allowedlist-distribution

<table>
<thead>
<tr>
<th>Packets</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0-3]</td>
<td>0</td>
</tr>
<tr>
<td>[4-7]</td>
<td>0</td>
</tr>
<tr>
<td>[8-15]</td>
<td>0</td>
</tr>
<tr>
<td>[16-31]</td>
<td>0</td>
</tr>
<tr>
<td>[32-63]</td>
<td>0</td>
</tr>
<tr>
<td>[64-127]</td>
<td>0</td>
</tr>
<tr>
<td>[128-255]</td>
<td>0</td>
</tr>
<tr>
<td>[256-511]</td>
<td>0</td>
</tr>
<tr>
<td>[512-1023]</td>
<td>0</td>
</tr>
<tr>
<td>[1024 and above]</td>
<td>0</td>
</tr>
</tbody>
</table>
show asp table arp

To debug the accelerated security path ARP tables, use the `show asp table arp` command.

```
show asp table arp  [interface  interface_name]  [address  ip_address  [netmask  mask]]
```

**Syntax Description**

- `address ip_address` (Optional) Identifies an IP address for which you want to view ARP table entries.
- `interface interface_name` (Optional) Identifies a specific interface for which you want to view the ARP table.
- `netmask mask` (Optional) Sets the subnet mask for the IP address.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show arp` command shows the contents of the control plane, while the `show asp table arp` command shows the contents of the accelerated security path, which might help you troubleshoot a problem. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

**Examples**

The following is sample output from the `show asp table arp` command:

```
> show asp table arp
Context: single_vf, Interface: inside
  10.86.194.50          Active  000f.66ce.5d46 hits 0
  10.86.194.1           Active  00b0.64ea.91a2 hits 638
  10.86.194.172         Active  0001.03cf.9e79 hits 0
  10.86.194.204         Active  000f.66ce.5d3c hits 0
  10.86.194.188         Active  000f.904b.80d7 hits 0
Context: single_vf, Interface: identity
  ::                        Active  0000.0000.0000 hits 0
  0.0.0.0                  Active  0000.0000.0000 hits 50208
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show arp</td>
<td>Shows the ARP table.</td>
</tr>
<tr>
<td>show arp statistics</td>
<td>Shows ARP statistics.</td>
</tr>
</tbody>
</table>
show asp table classify

To debug the accelerated security path classifier tables, use the `show asp table classify` command.

```
show asp table classify [interface interface_name] [crypto | domain domain_name] [hits] [match regexp]
```

**Syntax Description**

- **crypto** (Optional) Shows the encrypt, decrypt, and ipsec tunnel flow domains only.
- **domain domain_name** (Optional) Shows entries for a specific classifier domain. See the CLI help for a list of the available domains.
- **hits** (Optional) Shows classifier entries that have non-zero hits values.
- **interface interface_name** (Optional) Identifies a specific interface for which you want to view the classifier table.
- **match regexp** (Optional) Shows classifier entries that match the regular expression. Use quotes when regular expressions include spaces.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show asp table classify` command shows the classifier contents of the accelerated security path, which might help you troubleshoot a problem. The classifier examines properties of incoming packets, such as protocol, and source and destination address, to match each packet to an appropriate classification rule. Each rule is labeled with a classification domain that determines what types of actions are performed, such as dropping a packet or allowing it through. The information shown is used for debugging purposes only, and the output is subject to change. Consult Cisco TAC to help you debug your system with this command.

**Examples**

The following is sample output from the `show asp table classify` command:

```
> show asp table classify
Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in id=0x36f3800, priority=10, domain=punt, deny=false
   hits=0, user_data=0x0, flags=0x0
   src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip=10.86.194.60, mask=255.255.255.255, port=0, tag=any
in id=0x33d3508, priority=99, domain=inspect, deny=false
   hits=0, user_data=0x0, use_real_addr, flags=0x0
   src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
in id=0x33d3978, priority=99, domain=inspect, deny=false
   hits=0, user_data=0x0, use_real_addr, flags=0x0
   src ip=0.0.0.0, mask=0.0.0.0, port=53, tag=any
   dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
...
The following is sample output from the `show asp table classify hits` command with a record of the last clearing hits counters:

**Interface mgmt:**
```
in id=0x494cd88, priority=210, domain=permit, deny=true
  hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
  mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
  dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
  hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
  mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
```

**Interface inside:**
```
in id=0x48f1580, priority=210, domain=permit, deny=true
  hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
  mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
  dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
  hits=101, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
  mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
```

**Interface outside:**
```
in id=0x48c0970, priority=210, domain=permit, deny=true
  hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
  mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
  dscp=0x0
```

The following is sample output from the `show asp table classify hits` command that includes Layer 2 information:

**Input Table**
```
in id=0x7fff2de10ae0, priority=120, domain=permit, deny=false
  hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1
  src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0
  dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, dscp=0x0
  input_ifc=LAN-SEGMENT, output_ifc=identity
in id=0x7fff2de135c0, priority=0, domain=inspect-ip-options, deny=true
  hits=41, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
  input_ifc=LAN-SEGMENT, output_ifc=any
...```

**Output Table:**
```
L2 - Input Table:
```
in id=0x7fff2de0e080, priority=120, domain=permit, deny=false
  hits=30, user_data=0x0, cs_id=0x0, l3_type=0x608
  src mac=0000.0000.0000, mask=0000.0000.0000
  dst mac=0000.0000.0000, mask=0000.0000.0000
  input_ifc=LAN-SEGMENT, output_ifc=any
in id=0x7fff2de0f800, priority=1, domain=permit, deny=false
  hits=382, user_data=0x0, cs_id=0x0, l3_type=0x8
  src mac=0000.0000.0000, mask=0000.0000.0000
  dst mac=0000.0000.0000, mask=0000.0000.0000
  input_ifc=LAN-SEGMENT, output_ifc=any
in id=0x7fff2de0e800, priority=1, domain=permit, deny=false
  hits=312, user_data=0x0, cs_id=0x0, l3_type=0x8
  src mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
  dst mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
```
input_ifc=LAN-SEGMENT, output_ifc=any
show asp table cluster chash-table

To debug the accelerated security path cHash tables for clustering, use the `show asp table cluster chash-table` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `show asp table cluster chash-table` command shows the contents of the accelerated security path, which might help you troubleshoot a problem. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

### Examples

The following is sample output from the `show asp table cluster chash-table` command:

```
> show asp table cluster chash-table
Cluster current chash table:

00003333 21001200 22000033 02222223 33331111 21110000 00133103 22222223 30000102 11222222 23222331 00002223
(...output truncated...)
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show asp cluster counter</code></td>
<td>Shows cluster datapath counter information.</td>
</tr>
</tbody>
</table>
show asp table interfaces

To debug the accelerated security path interface tables, use the **show asp table interfaces** command.

**show asp table interfaces**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **show asp table interfaces** command shows the interface table contents of the accelerated security path, which might help you troubleshoot a problem. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

**Examples**

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

```bash
> show asp table interfaces
** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd, 0x0040-RPF Enabled
Soft-np interface 'dmz' is up
  context single_vf, nicnum 0, mtu 1500
  vlan 300, Not shared, seclvl 50
  0 packets input, 1 packets output
  flags 0x20
Soft-np interface 'foo' is down
  context single_vf, nicnum 2, mtu 1500
  vlan <None>, Not shared, seclvl 0
  0 packets input, 0 packets output
  flags 0x20
Soft-np interface 'outside' is down
  context single_vf, nicnum 1, mtu 1500
  vlan <None>, Not shared, seclvl 50
  0 packets input, 0 packets output
  flags 0x20
Soft-np interface 'inside' is up
  context single_vf, nicnum 0, mtu 1500
  vlan <None>, Not shared, seclvl 100
  680277 packets input, 92501 packets output
  flags 0x20
```

...
show asp table routing

To debug the accelerated security path routing tables, use the `show asp table routing` command. This command supports IPv4 and IPv6 addresses.

```
show asp table routing [management-only] [input | output] [address ip_address [netmask mask]] | interface interface_name
```

**Syntax Description**

- **address ip_address**
  - Sets the IP address for which you want to view routing entries. For IPv6 addresses, you can include the subnet mask as a slash (/) followed by the prefix (0 to 128). For example, enter fe80::2e0:b6ff:fe01:3b7a/128.

- **input**
  - Shows the entries from the input route table.

- **interface interface_name**
  - (Optional) Identifies a specific interface for which you want to view the routing table.

- **netmask mask**
  - For IPv4 addresses, specifies the subnet mask.

- **output**
  - Shows the entries from the output route table.

- **management-only**
  - Shows the number portability routes in the management routing table.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show asp table routing` command shows the routing table contents of the accelerated security path, which might help you troubleshoot a problem. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command. The management-only keyword, displays the number-portability routes in the management routing table.

**Examples**

The following is sample output from the `show asp table routing` command:

```
show asp table routing

in 255.255.255.255 255.255.255.255 identity
in 224.0.0.9 255.255.255.255 identity
in 10.86.194.60 255.255.255.255 identity
in 10.86.195.255 255.255.255.255 identity
in 10.86.194.0 255.255.255.255 identity
in 209.165.202.159 255.255.255.255 identity
in 209.165.202.255 255.255.255.255 identity
in 209.165.201.30 255.255.255.255 identity
in 209.165.201.0 255.255.255.255 identity
in 10.86.194.0 255.255.254.0 inside
in 224.0.0.0 240.0.0.0 identity
in 0.0.0.0 0.0.0.0 inside
out 255.255.255.255 255.255.255.255 foo
out 224.0.0.0 240.0.0.0 foo
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show route</code></td>
<td>Shows the routing table in the control plane.</td>
</tr>
</tbody>
</table>
show asp table socket

To help debug the accelerated security path socket information, use the `show asp table socket` command.

```
show asp table socket [handle] [stats]
```

**Syntax Description**

- **handle**: Specifies the length of the socket.
- **stats**: Shows the statistics from the accelerated security path socket table.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show asp table socket` command shows the accelerated security path socket information, which might help in troubleshooting accelerated security path socket problems. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

**Examples**

The following is sample output from the `show asp table socket` command.

```
Protocol  Socket  Local Address  Foreign Address  State
TCP       00012bac 10.86.194.224:23 0.0.0.0:* LISTEN
TCP       0001c124 10.86.194.224:22 0.0.0.0:* LISTEN
SSL       00023b84 10.86.194.224:443 0.0.0.0:* LISTEN
SSL       0002d01c 192.168.1.1:443 0.0.0.0:* LISTEN
DTLS      00032bic 10.86.194.224:443 0.0.0.0:* LISTEN
SSL       0003a3d4 0.0.0.0:443 0.0.0.0:* LISTEN
DTLS      00046074 0.0.0.0:443 0.0.0.0:* LISTEN
TCP       02c08aec 10.86.194.224:22 171.69.137.139:4190 ESTAB
```

The following is sample output from the `show asp table socket stats` command.

```
TCP Statistics:
  Rcvd:
    checksum errors 0
    no port 0
  Sent:
    total 0
UDP Statistics:
  Rcvd:
    checksum errors 0
  Sent:
    total 0
    copied 0
NP SSL System Stats:
  Handshake Started: 33
  Handshake Complete: 33
  SSL Open: 4
```
SSL Close: 117
SSL Server: 58
SSL Server Verify: 0
SSL Client: 0

TCP/UDP statistics are packet counters representing the number of packets sent or received that are directed to a service that is running or listening on the device, such as Telnet, SSH, or HTTPS. Checksum errors are the number of packets dropped because the calculated packet checksum did not match the checksum value stored in the packet (that is, the packet was corrupted). The NP SSL statistics indicate the number of each type of message received. Most indicate the start and completion of new SSL connections to either the SSL server or SSL client.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show asp table vpn-context</td>
<td>Shows the accelerated security path VPN context tables.</td>
</tr>
</tbody>
</table>
show asp table vpn-context

To debug the accelerated security path VPN context tables, use the `show asp table vpn-context` command.

```
show asp table vpn-context [detail]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Shows additional detail for the VPN context tables.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show asp table vpn-context` command shows the VPN context contents of the accelerated security path, which might help you troubleshoot a problem. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

**Examples**

The following is sample output from the `show asp table vpn-context` command:

```
> show asp table vpn-context
VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=00000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=00000305043, rk=00000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=00000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=00000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=00000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=00000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=00000000061, gc=2
...
```

The following is sample output from the `show asp table vpn-context` command when the persistent IPsec tunnelled flows feature is enabled, as shown by the PRESERVE flag:

```
> show asp table vpn-context
VPN Ctx=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000, gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000, gc=0
```

The following is sample output from the `show asp table vpn-context detail` command. When the persistent IPsec tunnelled flows feature is enabled, the flags will include the PRESERVE flag.

```
> show asp table vpn-context detail
VPN Ctx=0058070576 [0x03761630]
State=UP
Flags=DECR+ESP
SA=0x037928F0
SPI=0xEA0F21F0
```
Group = 0
Pkts = 0
Bad Pkts = 0
Bad SPI = 0
Spoof = 0
Bad Crypto = 0
Rekey Pkt = 0
Rekey Call = 0

VPN Ctx = 0058193920 [0x0377F800]
State = UP
Flags = ENCR+ESP
SA = 0x037B4B70
SPI = 0x900FDC32
Group = 0
Pkts = 0
Bad Pkts = 0
Bad SPI = 0
Spoof = 0
Bad Crypto = 0
Rekey Pkt = 0
Rekey Call = 0

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show asp drop</td>
<td>Shows the accelerated security path counters for dropped packets.</td>
</tr>
</tbody>
</table>
show asp table zone

To debug the accelerated security path zone table, use the `show asp table zone` command.

**show asp table zone**

---

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The `show asp table zone` command shows the contents of the accelerated security path, which might help you troubleshoot a problem. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

---

**Examples**

The following is sample output from the `show asp table zone` command. In this example, the zone named is-154 is actually an inline set, not a traffic zone.

```
> show asp table zone
Zone: krjones-passive-security-zone id: 48947
    Security-level: 0
    Context : single_vf
    Zone member(s):
        passive GigabitEthernet0/0

Zone: passive_default_context_0 id: 1
    Security-level: 0
    Context : single_vf
    Zone member(s):

Zone: is-154 id: 34309
    Security-level: 0
    Context : single_vf
    Zone member(s):
        out GigabitEthernet0/2
        in  GigabitEthernet0/1
```

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show inline-set</td>
<td>Shows the inline sets.</td>
</tr>
<tr>
<td>show zone</td>
<td>Shows the traffic zones.</td>
</tr>
</tbody>
</table>
show audit-log

To display the system audit log, use the `show audit-log` command.

```
> show audit-log
Audit Log Output:
  time : 1476223151 (Tue Oct 11 21:59:11 2016)
event_type : notify
subsystem : Task Queue
actor : System
message : Successful task completion : Clam update synchronization from firepower
result : Success
action_source_ip : localhost
action_destination_ip : localhost
----------------------------------------------------------
  time : 1476222646 (Tue Oct 11 21:50:46 2016)
event_type : notify
subsystem : Task Queue
actor : System
message : Successful task completion : Apply AMP Dynamic Analysis Configuration from firepower
result : Success
action_source_ip : localhost
action_destination_ip : localhost
----------------------------------------------------------
  time : 1476222564 (Tue Oct 11 21:49:24 2016)
event_type : notify
subsystem : Task Queue
actor : System
message : Successful task completion : Apply Initial Health Policy 2016-10-11 18:54:59 from firepower
result : Success
action_source_ip : localhost
action_destination_ip : localhost
----------------------------------------------------------
  time : 1476222563 (Tue Oct 11 21:49:23 2016)
event_type : notify
subsystem : Health > Health Policy > Apply > Initial Health Policy 2016-10-20 18:18:34 from firepower
result : Success
action_source_ip : localhost
action_destination_ip : localhost
----------------------------------------------------------
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command displays the audit log in reverse chronological order; the most recent audit log events are listed first.

Events can include system updates, permission problems, configuration changes, and policy applications. The information is available for devices remotely managed by Firepower Management Center only. The audit log is empty for locally managed systems.

Examples

The following example shows the audit log.
show audit-log

16-10-11 18:54:59 > firepower
actor: admin
message: Apply
result: Success
action_source_ip: 127.0.0.1
action_destination_ip: localhost

----------------------------------------------------------
event_type: notify
subsystem: Task Queue
actor: System
message: Successful task completion: Registration '10.83.57.41'
result: Success
action_source_ip: localhost
action_destination_ip: localhost

----------------------------------------------------------
event_type: Restart
subsystem: NTP Configuration changed
actor: Default User
message: Restart
result: Success
action_source_ip: Default User IP
action_destination_ip: Default Target IP

----------------------------------------------------------
show b

- show banner, on page 354
- show bfd drops, on page 355
- show bfd map, on page 356
- show bfd neighbors, on page 357
- show bfd summary, on page 358
- show bgp, on page 360
- show bgp cidr-only, on page 366
- show bgp community, on page 367
- show bgp community-list, on page 368
- show bgp filter-list, on page 369
- show bgp injected-paths, on page 370
- show bgp ipv4 unicast, on page 371
- show bgp ipv6 unicast, on page 372
- show bgp ipv4/ipv6 unicast community, on page 374
- show bgp ipv4/ipv6 unicast community-list, on page 375
- show bgp ipv4/ipv6 unicast neighbors, on page 376
- show bgp ipv4/ipv6 unicast paths, on page 382
- show bgp ipv4/ipv6 unicast prefix-list, on page 383
- show bgp ipv4/ipv6 unicast regexp, on page 384
- show bgp ipv4/ipv6 unicast route-map, on page 385
- show bgp ipv4/ipv6 unicast summary, on page 386
- show bgp neighbors, on page 388
- show bgp paths, on page 397
- show bgp prefix-list, on page 398
- show bgp regexp, on page 399
- show bgp rib-failure, on page 400
- show bgp summary, on page 401
- show bgp update-group, on page 405
- show blocks, on page 408
- show bootvar, on page 412
- show bridge-group, on page 413
# show banner

To display the configured banner message, enter the **show banner** command.

```
show banner  [login]
```

## Syntax Description

| login | Displays the banner that has been set up for the password login prompt. |

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Examples

```
> show banner
```
show bfd drops

To display the number of dropped packets in BFD, use the `show bfd drops` command.

```
show bfd drops
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example displays the BFD dropped packets.

```
> show bfd drops
BFD Drop Statistics
IPV4 IPV6 IPV4-M IPV6-M
Invalid TTL 0 0 0 0
BFD Not Configured 0 0 0 0
No BFD Adjacency 0 0 0 0
Invalid Header Bits 0 0 0 0
Invalid Discriminator 0 0 0 0
Session AdminDown 0 0 0 0
Authen invalid BFD ver 0 0 0 0
Authen invalid len 0 0 0 0
Authen invalid seq 0 0 0 0
Authen failed 0 0 0 0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear bfd counters</td>
<td>Clears the BFD counters.</td>
</tr>
<tr>
<td>show bfd map</td>
<td>Displays the configured BFD maps.</td>
</tr>
<tr>
<td>show bfd neighbors</td>
<td>Displays a line-by-line listing of existing BFD adjacencies.</td>
</tr>
<tr>
<td>show bfd summary</td>
<td>Displays summary information for BFD.</td>
</tr>
</tbody>
</table>
**show bfd map**

To display the configured BFD maps, use the **show bfd map** command.

**show bfd map**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the BFD maps.

```shell
> show bfd map
Destination: 40.40.40.2/24
Source: 50.50.50.2/24
Template: mh
Authentication(Type): sha-1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear bfd counters</td>
<td>Clears the BFD counters.</td>
</tr>
<tr>
<td>show bfd drops</td>
<td>Displays the numbered of dropped packets in BFD.</td>
</tr>
<tr>
<td>show bfd neighbors</td>
<td>Displays a line-by-line listing of existing BFD adjacencies.</td>
</tr>
<tr>
<td>show bfd summary</td>
<td>Displays summary information for BFD.</td>
</tr>
</tbody>
</table>
show bfd neighbors

To display a line-by-line listing of existing BFD adjacencies, use the `show bfd neighbors` command.

```
show bfd neighbors [client bgp] [ipv4 [ip_address] | ipv6 [ipv6_address] | multihop-ipv4 [ip_address] | multihop-ipv6 [ipv6_address]] [inactive] [detail]
```

**Syntax Description**

- `client bgp` (Optional) Displays the neighbors of the BGP client.
- `ipv4 [ip_address]` (Optional) Displays single-hop IPv4 neighbors. You can optionally specify a particular neighbor address.
- `ipv6 [ipv6_address]` (Optional) Displays single-hop IPv6 neighbors. You can optionally specify a particular neighbor address.
- `multihop-ipv4 [ip_address]` (Optional) Displays multi-hop IPv4 neighbors. You can optionally specify a particular neighbor address.
- `multihop-ipv6 [ipv6_address]` (Optional) Displays multi-hop IPv6 neighbors. You can optionally specify a particular neighbor address.
- `inactive` (Optional) Displays the inactive adjacencies.
- `detail` (Optional) Displays all BFD protocol parameters and timers for each neighbor.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the BFD neighbors.

```
> show bfd neighbors
OurAddr NeighAddr LD/RD RH Holdown(mult) State Int
172.16.10.1 172.16.10.2 1/6 1 260 (3 ) Up Fa0/1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear bfd counters</code></td>
<td>Clears the BFD counters.</td>
</tr>
<tr>
<td><code>show bfd drops</code></td>
<td>Displays the number of dropped packets in BFD.</td>
</tr>
<tr>
<td><code>show bfd map</code></td>
<td>Displays the configured BFD maps.</td>
</tr>
<tr>
<td><code>show bfd summary</code></td>
<td>Displays summary information for BFD.</td>
</tr>
</tbody>
</table>
show bfd summary

To display summary information for BFD, use the `show bfd summary` command.

```
show bfd summary [client | session]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>(Optional) Displays the BFD summary for clients.</td>
</tr>
<tr>
<td>session</td>
<td>(Optional) Displays the BFD summary for sessions.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to display summary information about BFD, BFD clients, or BFD sessions. When a BFD client launches a session with a peer, BFD sends periodic BFD control packets to the peer. Information about the following states of a session are included in the output of this command:

- **Up**—When another BFD interface acknowledges the BFD control packets, the session moves into an Up state.
- **Down**—The session and the data path are declared down if a data path failure occurs and BFD does not receive a control packet within the configured amount of time. When a session is down, BFD notifies the BFD client so that the client can perform necessary actions to reroute the traffic.

### Examples

The following example displays the BFD summaries.

```
> show bfd summary
Session Up Down
Total 1 1 0

> show bfd summary session
Protocol Session Up Down
IPV4 1 1 0
Total 1 1 0

> show bfd summary client
Client Session Up Down
BGP 1 1 0
EIGRP 1 1 0
Total 2 2 0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear bfd counters</td>
<td>Clears the BFD counters.</td>
</tr>
<tr>
<td>show bfd drops</td>
<td>Displays the numbered of dropped packets in BFD.</td>
</tr>
<tr>
<td>show bfd map</td>
<td>Displays the configured BFD maps.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>show bfd neighbors</td>
<td>Displays a line-by-line listing of existing BFD adjacencies.</td>
</tr>
</tbody>
</table>
show bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the `show bgp` command.

```plaintext
show bgp [ip-address] [mask] [longer-prefixes] [injected] | shorter-prefixes [length] | bestpath
| multipaths | subnets] | bestpath | multipaths] | all | prefix-list name | pending-prefixes
| route-map name ]
```

**Syntax Description**

- `ip-address` (Optional) Specifies the network in the BGP routing table to display.
- `mask` (Optional) Mask to filter or match hosts that are part of the specified network.
- `longer-prefixes` (Optional) Displays the specified route and all more specific routes.
- `injected` (Optional) Displays more specific prefixes injected into the BGP routing table.
- `shorter-prefixes` (Optional) Displays the specified route and all less specific routes.
- `length` (Optional) The prefix length. The value for this argument is a number from 0 to 32.
- `bestpath` (Optional) Displays the bestpath for this prefix.
- `multipaths` (Optional) Displays multipaths for this prefix.
- `subnets` (Optional) Displays the subnet routes for the specified prefix.
- `all` (Optional) Displays all address family information in the BGP routing table.
- `prefix-list name` (Optional) Filters the output based on the specified prefix list.
- `pending-prefixes` (Optional) Displays prefixes that are pending deletion from the BGP routing table.
- `route-map name` (Optional) Filters the output based on the specified route map.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show bgp` command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.

**Examples**

The following sample output shows the BGP routing table:

```plaintext
> show bgp
BGP table version is 22, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```
The following table explains each field.

**Table 3: show bgp Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• s—The table entry is suppressed.</td>
</tr>
<tr>
<td></td>
<td>• d—The table entry is dampened.</td>
</tr>
<tr>
<td></td>
<td>• h—The table entry history.</td>
</tr>
<tr>
<td></td>
<td>• *—The table entry is valid.</td>
</tr>
<tr>
<td></td>
<td>• &gt;—The table entry is the best entry to use for that network.</td>
</tr>
<tr>
<td></td>
<td>• i—The table entry was learned via an internal BGP (iBGP) session.</td>
</tr>
<tr>
<td></td>
<td>• r—The table entry is a RIB-failure.</td>
</tr>
<tr>
<td></td>
<td>• S—The table entry is stale.</td>
</tr>
<tr>
<td></td>
<td>• m—The table entry has multipath to use for that network.</td>
</tr>
<tr>
<td></td>
<td>• b—The table entry has backup path to use for that network.</td>
</tr>
<tr>
<td></td>
<td>• x—The table entry has best external route to use for the network.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Origin codes</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised.</td>
</tr>
<tr>
<td></td>
<td>• e—Entry originated from an Exterior Gateway Protocol (EGP).</td>
</tr>
<tr>
<td></td>
<td>• ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, the value of the interautonomous system metric.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
<tr>
<td>(stale)</td>
<td>Indicates that the following path for the specified autonomous system is marked as “stale” during a graceful restart process.</td>
</tr>
</tbody>
</table>

The following sample output displays information about the 192.168.1.0 entry in the BGP routing table:

```bash
> show bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
  3
    10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
    10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best, recursive-via-connected
```

The following sample output displays information about the 10.3.3.3 255.255.255.255 entry in the BGP routing table:

```bash
> show bgp 10.3.3.3 255.255.255.255
BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
  Multipath: eBGP
  Flag: 0x860
  Advertised to update-groups:
    1
    200
```
The following table explains each field.

**Table 4: show bgp (4 byte autonomous system numbers) Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP routing table entry for</td>
<td>IP address or network number of the routing table entry.</td>
</tr>
<tr>
<td>version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>Paths</td>
<td>The number of available paths, and the number of installed best paths. This line displays “Default-IP-Routing-Table” when the best path is installed in the IP routing table.</td>
</tr>
<tr>
<td>Multipath</td>
<td>This field is displayed when multipath loadsharing is enabled. This field will indicate if the multipaths are iBGP or eBGP.</td>
</tr>
<tr>
<td>Advertised to update-groups</td>
<td>The number of each update group for which advertisements are processed.</td>
</tr>
<tr>
<td>Origin</td>
<td>Origin of the entry. The origin can be IGP, EGP, or incomplete. This line displays the configured metric (0 if no metric is configured), the local preference value (100 is default), and the status and type of route (internal, external, multipath, best).</td>
</tr>
<tr>
<td>Extended Community</td>
<td>This field is displayed if the route carries an extended community attribute. The attribute code is displayed on this line. Information about the extended community is displayed on a subsequent line.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show bgp` command entered with the `all` keyword.

Information about all configured address families is displayed.

> show bgp all

For address family: IPv4 Unicast

BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>10.13.13.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>10.15.15.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
</tbody>
</table>
The following is sample output from the `show bgp` command entered with the longer-prefixes keyword:

```plaintext
> show bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.92.0.0</td>
<td>10.92.72.30</td>
<td>8896</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>* 10.92.1.0</td>
<td>10.92.72.30</td>
<td>8796</td>
<td>32768</td>
<td>0</td>
<td>109 108  ?</td>
</tr>
<tr>
<td>* 10.92.11.0</td>
<td>10.92.72.30</td>
<td>42482</td>
<td>32768</td>
<td>0</td>
<td>109 108  ?</td>
</tr>
<tr>
<td>* 10.92.14.0</td>
<td>10.92.72.30</td>
<td>8796</td>
<td>32768</td>
<td>0</td>
<td>109 108  ?</td>
</tr>
<tr>
<td>* 10.92.15.0</td>
<td>10.92.72.30</td>
<td>8696</td>
<td>32768</td>
<td>0</td>
<td>109 108  ?</td>
</tr>
<tr>
<td>* 10.92.16.0</td>
<td>10.92.72.30</td>
<td>1400</td>
<td>32768</td>
<td>0</td>
<td>109 108  ?</td>
</tr>
<tr>
<td>* 10.92.17.0</td>
<td>10.92.72.30</td>
<td>1400</td>
<td>32768</td>
<td>0</td>
<td>109 108  ?</td>
</tr>
<tr>
<td>* 10.92.18.0</td>
<td>10.92.72.30</td>
<td>8876</td>
<td>32768</td>
<td>0</td>
<td>109 108  ?</td>
</tr>
<tr>
<td>* 10.92.19.0</td>
<td>10.92.72.30</td>
<td>8876</td>
<td>32768</td>
<td>0</td>
<td>109 108  ?</td>
</tr>
<tr>
<td>* 10.92.20.0</td>
<td>10.92.72.30</td>
<td>8876</td>
<td>32768</td>
<td>0</td>
<td>109 108  ?</td>
</tr>
</tbody>
</table>
```

The following is sample output from the `show bgp` command entered with the shorter-prefixes keyword. An 8-bit prefix length is specified.

```plaintext
> show bgp 172.16.0.0/16 shorter-prefixes 8

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 172.16.0.0</td>
<td>10.0.0.2</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>?</td>
</tr>
<tr>
<td>* 10.0.0.2</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

The following is sample output from the `show bgp` command entered with the prefix-list keyword:

```plaintext
> show bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
```
The following is sample output from the `show bgp` command entered with the `route-map` keyword:

```plaintext
> show bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 192.168.1.0</td>
<td>10.0.0.2</td>
<td>0</td>
<td></td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>10.0.0.2</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>?</td>
</tr>
</tbody>
</table>
```
show bgp cidr-only

To display routes with classless inter domain routing (CIDR), use the `show bgp cidr-only` command.

```
show bgp cidr-only
```

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bgp cidr-only` command. For an explanation of the output, see the `show bgp` command.

```
> show bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 192.168.0.0/8</td>
<td>172.16.72.24</td>
<td>0</td>
<td>1878</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*&gt; 172.16.0.0/16</td>
<td>172.16.72.30</td>
<td>0</td>
<td>108</td>
<td>?</td>
<td></td>
</tr>
</tbody>
</table>
```
show bgp community

To display routes that belong to specified BGP communities, use the `show bgp community` command.

**Syntax**

```
show bgp community [community-number] [exact-match] [no-advertise] [no-export]
```

**Syntax Description**

- **community-number** (Optional) Valid value is a community number in the range from 1 to 4294967295 or AA:NN (autonomous system-community number:2-byte number).
- **exact-match** (Optional) Displays only routes that have an exact match.
- **no-advertise** (Optional) Displays only routes that are not advertised to any peer (well-known community).
- **no-export** (Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bgp community` command. For an explanation of the output, see the `show bgp` command.

```plaintext
> show bgp community 111:12345
BGP table version is 10, local router ID is 224.0.0.10
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
*> 172.16.2.2/32  10.43.222.2      0       0       222  ?
*> 10.0.0.0       10.43.222.2      0       0       222  ?
*> 10.43.0.0      10.43.222.2      0       0       222  ?
*> 10.43.44.44/32 10.43.222.2      0       0       222  ?
*> 10.43.222.0/24 10.43.222.2      0       0       222  i
*> 172.17.240.0/21 10.43.222.2      0       0       222  ?
*> 192.168.212.0  10.43.222.2      0       0       222  i
*> 172.31.1.0     10.43.222.2      0       0       222  ?
```
**show bgp community-list**

To display routes that are permitted by the Border Gateway Protocol (BGP) community list, use the `show bgp community-list` command.

```
show bgp community-list {community-list-number | community-list-name [exact-match]}
```

**Syntax Description**

- **community-list-number**: A standard or expanded community list number in the range from 1 to 500.
- **community-list-name**: Community list name. The community list name can be standard or expanded.
- **exact-match**: (Optional) Displays only routes that have an exact match.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output of the `show bgp community-list`. For an explanation of the output, see the `show bgp` command.

```
> show bgp community-list 20
BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.3.0.0</td>
<td>10.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 1239 ?</td>
</tr>
<tr>
<td>* 10.16.0.0</td>
<td>10.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 1239 ?</td>
</tr>
<tr>
<td>* 10.6.0.0</td>
<td>10.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 568 ?</td>
</tr>
<tr>
<td>* 10.16.0.0</td>
<td>10.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 568 ?</td>
</tr>
<tr>
<td>* 10.7.0.0</td>
<td>10.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 35 ?</td>
</tr>
<tr>
<td>* 10.16.0.0</td>
<td>10.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 35 ?</td>
</tr>
</tbody>
</table>
```

Cisco Firepower Threat Defense Command Reference
show bgp filter-list

To display routes that conform to a specified filter list, use the show bgp filter-list command.

**show bgp filter-list access-list-name**

**Syntax Description**

| access-list-name | Name of an autonomous system path access list. Valid values are from 1 to 500. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output of the show bgp filter-list command. For an explanation of the output, see the show bgp command.

```plaintext
> show bgp filter-list filter-list-acl
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
* 172.16.0.0 172.16.72.30 0 109 108 ?
* 172.16.1.0 172.16.72.30 0 109 108 ?
* 172.16.11.0 172.16.72.30 0 109 108 ?
* 172.16.14.0 172.16.72.30 0 109 108 ?
* 172.16.15.0 172.16.72.30 0 109 108 ?
* 172.16.16.0 172.16.72.30 0 109 108 ?
* 172.16.17.0 172.16.72.30 0 109 108 ?
* 172.16.18.0 172.16.72.30 0 109 108 ?
* 172.16.19.0 172.16.72.30 0 109 108 ?
* 172.16.24.0 172.16.72.30 0 109 108 ?
* 172.16.29.0 172.16.72.30 0 109 108 ?
* 172.16.30.0 172.16.72.30 0 109 108 ?
* 172.16.33.0 172.16.72.30 0 109 108 ?
* 172.16.35.0 172.16.72.30 0 109 108 ?
* 172.16.36.0 172.16.72.30 0 109 108 ?
* 172.16.37.0 172.16.72.30 0 109 108 ?
* 172.16.38.0 172.16.72.30 0 109 108 ?
* 172.16.39.0 172.16.72.30 0 109 108 ?
```
show bgp injected-paths

To display all the injected paths in the Border Gateway Protocol (BGP) routing table, use the `show bgp injected-paths` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show bgp injected-paths` command. For an explanation of the output, see the `show bgp` command.

```
> show bgp injected-paths
BGP table version is 11, local router ID is 10.0.0.1
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
*  >  172.16.0.0     10.0.0.2        0    0    0
*  >  172.17.0.0/16  10.0.0.2        0    0    0
```
show bgp ipv4 unicast

To display entries in the IP version 4 (IPv4) Border Gateway Protocol (BGP) routing table, use the `show bgp ipv4 unicast` command.

```
show bgp ipv4 unicast  [cidr-only]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>unicast</strong></td>
</tr>
<tr>
<td><strong>cidr-only</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>6.1</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bgp ipv4 unicast` command: For an explanation of the output, see the `show bgp` command.

```shell
> show bgp ipv4 unicast
BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.10.0.24</td>
<td>172.16.10.1</td>
<td>0</td>
<td>0</td>
<td>300</td>
<td>i</td>
</tr>
<tr>
<td>* 10.10.20.0/24</td>
<td>172.16.10.1</td>
<td>0</td>
<td>0</td>
<td>300</td>
<td>i</td>
</tr>
<tr>
<td>* 10.20.10.0/24</td>
<td>172.16.10.1</td>
<td>0</td>
<td>0</td>
<td>300</td>
<td>i</td>
</tr>
</tbody>
</table>
```
show bgp ipv6 unicast

To display entries in the IPv6 Border Gateway Protocol (BGP) routing table, use the `show bgp ipv6` command.

```
show bgp ipv6 unicast [ipv6-prefix/prefix-length] [longer-prefixes] [labels]
```

**Syntax Description**

- `unicast` (Optional) Specifies IPv6 unicast address prefixes.

- `ipv6-prefix` (Optional) IPv6 network number, entered to display a particular network in the IPv6 BGP routing table.
  
  This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

- `/prefix-length` (Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

- `longer-prefixes` (Optional) Displays the route and more specific routes.

- `labels` (Optional) Displays the policies applied to this neighbor per address family.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bgp ipv6 unicast` command, showing information for prefix 3FFE:500::/24. For an explanation of the output, see the `show bgp` command.

```
> show bgp ipv6 unicast 3FFE:500::/24
BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
    293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
    Origin IGP, localpref 100, valid, external, best
    4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
    Origin IGP, metric 1, localpref 100, valid, external
    33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
    Origin IGP, localpref 100, valid, external
    6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
    Origin IGP, localpref 100, valid, external
    1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
    Origin IGP, localpref 100, valid, external
    237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
    Origin IGP, localpref 100, valid, external
> show bgp ipv6 unicast
```
BGP table version is 28, local router ID is 172.10.10.1

Status codes: s suppressed, h history, * valid, > best, i - internal,
           r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt;4004::/64</td>
<td>::FFFF:172.11.11.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* i</td>
<td>::FFFF:172.30.30.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>
**show bgp ipv4/ipv6 unicast community**

To display entries in the IPv4 or IPv6 Border Gateway Protocol (BGP) routing table, use the `show bgp ipv4 unicast community` or `show bgp ipv6 unicast community` command respectively.

```plaintext
show bgp {ipv4 | ipv6} unicast community [community-number] [exact-match] [local-as | no-advertise | no-export]
```

**Syntax Description**

- **unicast**: Specifies IPv4 or IPv6 unicast address prefixes.
- **community-number**: (Optional) Valid value is a community number in the range from 1 to 4294967295 or AA:NN (autonomous system-community number:2-byte number).
- **exact-match**: (Optional) Displays only routes that have an exact match.
- **local-as**: (Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
- **no-advertise**: (Optional) Displays only routes that are not advertised to any peer (well-known community).
- **no-export**: (Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bgp ipv6 unicast community` command. For an explanation of the output, see the `show bgp` command.

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric  LocPrf  Weight  Path
*> 2001::0DB8:0:1::1/64 ::          0 32768 1
*> 2001::0DB8:0:1::1/80 ::          0 32768 ?
*> 2001::0DB8:0:2::/64 2001::0DB8:0:3::2 0 2 ?
*> 2001::0DB8:0:2:1::/80 2001::0DB8:0:3::2 0 2 ?
*> 2001::0DB8:0:3::1/64 2001::0DB8:0:3::2 0 2 ?
*> ::          0 32768 ?
*> 2001::0DB8:0:4::/64 2001::0DB8:0:3::2 0 2 ?
*> 2001::0DB8:0:5::1/64 ::          0 32768 ?
*> 2001::0DB8:0:6::/64 2000:0:0:3::2 0 2 3 ?
*> 2010::/64 ::          0 32768 ?
*> 2020::/64 ::          0 32768 ?
*> 2030::/64 ::          0 32768 ?
*> 2040::/64 ::          0 32768 ?
*> 2050::/64 ::          0 32768 ?
```
show bgp ipv4/ipv6 unicast community-list

To display routes that are permitted by the IPv4 or IPv6 Border Gateway Protocol (BGP) community list, use the show bgp ipv4 unicast community-list or show bgp ipv6 unicast community-list command respectively.

```
show bgp (ipv4 | ipv6) unicast community-list {number | name} [exact-match]
```

**Syntax Description**

- `unicast`: Specifies IPv4 or IPv6 unicast address prefixes.
- `number`: Community list number in the range from 1 to 199.
- `name`: Community list name.
- `exact-match`: (Optional) Displays only routes that have an exact match.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output of the `show bgp ipv6 unicast community-list` command for community list number 3. For an explanation of the output, see the `show bgp` command.

```
> show bgp ipv6 unicast community-list 3
BGP table version is 14, local router ID is 10.2.64.6
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 2001:0DB8::1::/64</td>
<td>2001:0DB8:0:3::1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>i</td>
</tr>
<tr>
<td>* 2001:0DB8::1::/80</td>
<td>2001:0DB8:0:3::1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>i</td>
</tr>
<tr>
<td>* 2001:0DB8::2::1/64</td>
<td>::</td>
<td>0</td>
<td>32768</td>
<td>1</td>
<td>i</td>
</tr>
<tr>
<td>* 2001:0DB8::2::1::/80</td>
<td>::</td>
<td>0</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>* 2001:0DB8::3::2/64</td>
<td>2001:0DB8:0:3::1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>* 2001:0DB8::3::2::/80</td>
<td>::</td>
<td>0</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>* 2001:0DB8::4::2/64</td>
<td>::</td>
<td>0</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>* 2001:0DB8::4::2::/64</td>
<td>2001:0DB8:0:3::1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>* 2010::/64</td>
<td>2001:0DB8:0:3::1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>* 2020::/64</td>
<td>2001:0DB8:0:3::1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>* 2030::/64</td>
<td>2001:0DB8:0:3::1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>* 2040::/64</td>
<td>2001:0DB8:0:3::1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>* 2050::/64</td>
<td>2001:0DB8:0:3::1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>?</td>
</tr>
</tbody>
</table>
```
show bgp ipv4/ipv6 unicast neighbors

To display information about IPv4 or IPv6 Border Gateway Protocol (BGP) connections to neighbors, use the **show bgp ipv4 unicast neighbors** or **show bgp ipv6 neighbors** command.

**show bgp {ipv4 | ipv6} unicast neighbors [ip-address] [received-routes | routes | advertised-routes | paths regular-expression]**

**Syntax Description**

- **unicast** Specifies IPv4 or IPv6 unicast address prefixes.
- **ip-address** (Optional) Address of the IPv4 or IPv6 BGP-speaking neighbor. If you omit this argument, all IPv4 or IPv6 neighbors are displayed. IPv6 addresses must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
- **received-routes** (Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
- **routes** (Optional) Displays all routes received and accepted. This is a subset of the output from the received-routes keyword.
- **advertised-routes** (Optional) Displays all the routes the networking device advertised to the neighbor.
- **paths regular-expression** (Optional) Regular expression used to match the paths received.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show bgp ipv6 unicast neighbors
BGP neighbor is 3FFE:700:20:1::11, remote AS 65003, external link
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 31306 messages, 20 notifications, 0 in queue
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
  For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
```
Route map for outgoing advertisements is uni-out
77 accepted prefixes consume 4928 bytes
Prefix advertised 4303, suppressed 0, withdrawn 1328
Number of NLRIs in the update sent: max 1, min 0
1 history paths consume 64 bytes
Connections established 22; dropped 21
Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):

<table>
<thead>
<tr>
<th>Timer</th>
<th>Starts</th>
<th>Wakeups</th>
<th>Next</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrans</td>
<td>1218</td>
<td>5</td>
<td>0x0</td>
</tr>
<tr>
<td>TimeWait</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>AckHold</td>
<td>3327</td>
<td>3051</td>
<td>0x0</td>
</tr>
<tr>
<td>SendWnd</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>KeepAlive</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>GiveUp</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>PmtuAger</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>DeadWait</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
</tbody>
</table>

Iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354  sndwnd: 15531
Irs: 82133727  rcvnx: 821591465  rcvwnd: 15547  delrcvwnd: 837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
MinRTT: 8 ms, MaxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128

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

**Table 5: show bgp ipv4/ipv6 unicast neighbors fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.</td>
</tr>
<tr>
<td>remote AS</td>
<td>Autonomous system of the neighbor.</td>
</tr>
<tr>
<td>internal link</td>
<td>Indicates that this peer is an interior Border Gateway Protocol (iBGP) peer.</td>
</tr>
<tr>
<td>BGP version</td>
<td>BGP version being used to communicate with the remote router; the router ID (an IP address) of the neighbor is also specified.</td>
</tr>
<tr>
<td>remote router ID</td>
<td>A 32-bit number written as 4 octets separated by periods (dotted-decimal format).</td>
</tr>
<tr>
<td>BGP state</td>
<td>Internal state of this BGP connection.</td>
</tr>
<tr>
<td>up for</td>
<td>Amount of time that the underlying TCP connection has been in existence.</td>
</tr>
<tr>
<td>Last read</td>
<td>Time that BGP last read a message from this neighbor.</td>
</tr>
<tr>
<td>hold time</td>
<td>Maximum amount of time that can elapse between messages from the peer.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>keepalive interval</td>
<td>Time period between sending keepalive packets, which help ensure that the TCP connection is up.</td>
</tr>
<tr>
<td>Neighbor capabilities</td>
<td>BGP capabilities advertised and received from this neighbor.</td>
</tr>
<tr>
<td>Route refresh</td>
<td>Indicates that the neighbor supports dynamic soft reset using the route refresh capability.</td>
</tr>
<tr>
<td>Address family IPv6 Unicast</td>
<td>Indicates that BGP peers are exchanging IPv6 reachability information.</td>
</tr>
<tr>
<td>Received</td>
<td>Number of total BGP messages received from this peer, including keepalives.</td>
</tr>
<tr>
<td>notifications</td>
<td>Number of error messages received from the peer.</td>
</tr>
<tr>
<td>Sent</td>
<td>Total number of BGP messages that have been sent to this peer, including keepalives.</td>
</tr>
<tr>
<td>notifications</td>
<td>Number of error messages the router has sent to this peer.</td>
</tr>
<tr>
<td>advertisement runs</td>
<td>Value of the minimum advertisement interval.</td>
</tr>
<tr>
<td>For address family</td>
<td>Address family to which the following fields refer.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>neighbor version</td>
<td>Number used by the software to track the prefixes that have been sent and those that must be sent to this neighbor.</td>
</tr>
<tr>
<td>Route refresh request</td>
<td>Number of route refresh requests sent and received from this neighbor.</td>
</tr>
<tr>
<td>Community attribute (not shown in sample output)</td>
<td>Appears if the neighbor send-community command is configured for this neighbor.</td>
</tr>
<tr>
<td>Inbound path policy (not shown in sample output)</td>
<td>Indicates whether an inbound filter list or route map is configured.</td>
</tr>
<tr>
<td>Outbound path policy (not shown in sample output)</td>
<td>Indicates whether an outbound filter list, route map, or unsuppress map is configured.</td>
</tr>
<tr>
<td>bgp-in (not shown in sample output)</td>
<td>Name of the inbound update prefix filter list for the IPv6 unicast address family.</td>
</tr>
<tr>
<td>aggregate (not shown in sample output)</td>
<td>Name of the outbound update prefix filter list for the IPv6 unicast address family.</td>
</tr>
<tr>
<td>uni-out (not shown in sample output)</td>
<td>Name of the outbound route map for the IPv6 unicast address family.</td>
</tr>
<tr>
<td>accepted prefixes</td>
<td>Number of prefixes accepted.</td>
</tr>
<tr>
<td>Prefix advertised</td>
<td>Number of prefixes advertised.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>suppressed</td>
<td>Number of prefixes suppressed</td>
</tr>
<tr>
<td>withdrawn</td>
<td>Number of prefixes withdrawn.</td>
</tr>
<tr>
<td>history paths (not shown in sample output)</td>
<td>Number of path entries held to remember history.</td>
</tr>
<tr>
<td>Connections established</td>
<td>Number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other.</td>
</tr>
<tr>
<td>dropped</td>
<td>Number of times that a good connection has failed or been taken down.</td>
</tr>
<tr>
<td>Last reset</td>
<td>Elapsed time (in hours:minutes:seconds) since this peering session was last reset.</td>
</tr>
<tr>
<td>Connection state</td>
<td>State of the BGP Peer</td>
</tr>
<tr>
<td>unread input bytes</td>
<td>Number of bytes of packets still to be processed.</td>
</tr>
<tr>
<td>Local host, Local port</td>
<td>Peering address of the local router, plus the port.</td>
</tr>
<tr>
<td>Foreign host, Foreign port</td>
<td>Peering address of the neighbor.</td>
</tr>
<tr>
<td>Event Timers</td>
<td>Table that displays the number of starts and wakeups for each timer.</td>
</tr>
<tr>
<td>snduna</td>
<td>Last send sequence number for which the local host sent but has not received an acknowledgment.</td>
</tr>
<tr>
<td>sndnxt</td>
<td>Sequence number the local host will send next.</td>
</tr>
<tr>
<td>sndwnd</td>
<td>TCP window size of the remote host.</td>
</tr>
<tr>
<td>irs</td>
<td>Initial receive sequence number.</td>
</tr>
<tr>
<td>rcvnxt</td>
<td>Last receive sequence number the local host has acknowledged.</td>
</tr>
<tr>
<td>rcvwnd</td>
<td>TCP window size of the local host.</td>
</tr>
<tr>
<td>delrecvwnd</td>
<td>Delayed receive window--data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.</td>
</tr>
<tr>
<td>SRTT</td>
<td>A calculated smoothed round-trip timeout (in milliseconds).</td>
</tr>
<tr>
<td>RTTO</td>
<td>Round-trip timeout (in milliseconds).</td>
</tr>
<tr>
<td>RTV</td>
<td>Variance of the round-trip time (in milliseconds).</td>
</tr>
<tr>
<td>KRTT</td>
<td>New round-trip timeout (in milliseconds) using the Karn algorithm. This field separately tracks the round-trip time of packets that have been re-sent.</td>
</tr>
<tr>
<td>minRTT</td>
<td>Smallest recorded round-trip timeout (in milliseconds) with hard wire value used for calculation.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
---|---
maxRTT | Largest recorded round-trip timeout (in milliseconds).
ACK hold | Time (in milliseconds) the local host will delay an acknowledgment in order to “piggyback” data on it.
Flags | IP precedence of the BGP packets.
Datagrams: Rcvd | Number of update packets received from neighbor.
with data | Number of update packets received with data.
total data bytes | Total number of bytes of data.
Sent | Number of update packets sent.
with data | Number of update packets with data sent.
total data bytes | Total number of data bytes.

The following is sample output from the `show bgp ipv6 unicast neighbors` command with the `advertised-routes` keyword. For an explanation of the output, see the `show bgp` command.

```plaintext
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes
BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 2001:200::/35</td>
<td>3FFE:700:20:1::11</td>
<td>0</td>
<td>293</td>
<td>3425</td>
<td>2500</td>
</tr>
<tr>
<td>*&gt; 2001:208::/35</td>
<td>3FFE:C00:E:B::2</td>
<td>0</td>
<td>237</td>
<td>7610</td>
<td>i</td>
</tr>
<tr>
<td>*&gt; 2001:218::/35</td>
<td>3FFE:C00:E:C::2</td>
<td>0</td>
<td>3748</td>
<td>4697</td>
<td>i</td>
</tr>
</tbody>
</table>
```

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

```plaintext
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes
BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 2001:200::/35</td>
<td>3FFE:700:20:1::11</td>
<td>0</td>
<td>293</td>
<td>3425</td>
<td>2500</td>
</tr>
<tr>
<td>* 2001:208::/35</td>
<td>3FFE:700:20:1::11</td>
<td>0</td>
<td>293</td>
<td>7610</td>
<td>i</td>
</tr>
<tr>
<td>* 2001:218::/35</td>
<td>3FFE:700:20:1::11</td>
<td>0</td>
<td>293</td>
<td>3425</td>
<td>4697</td>
</tr>
<tr>
<td>* 2001:230::/35</td>
<td>3FFE:700:20:1::11</td>
<td>0</td>
<td>293</td>
<td>1275</td>
<td>3748</td>
</tr>
</tbody>
</table>
```

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

```plaintext
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
Address | Refcount | Metric | Path
0x6131D7DC | 2 | 0 | 293 3425 2500 i
0x6132861C | 2 | 0 | 293 7610 i
0x6131AD18 | 2 | 0 | 293 3425 4697 i
0x61324084 | 2 | 0 | 293 1275 3748 i
```
The table below describes the significant fields shown in the display.

### Table 6: `show bgp ipv6 neighbors paths fields`

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

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

```plaintext
� show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
BGP table version is 2443, local router ID is 192.168.0.2
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 2000:0:0:1::/64</td>
<td>2000:0:0:4::2</td>
<td>0 2 1 i</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2000:0:0:2::/64</td>
<td>2000:0:0:4::2</td>
<td>0 2 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2000:0:0:2:1::/80</td>
<td>2000:0:0:4::2</td>
<td>0 2 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2000:0:0:3::/64</td>
<td>2000:0:0:4::2</td>
<td>0 2 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2000:0:0:4::1/64</td>
<td>2000:0:0:4::2</td>
<td>0 2 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Cisco Firepower Threat Defense Command Reference
show bgp ipv4/ipv6 unicast paths

To display all the IPv4 or IPv6 Border Gateway Protocol (BGP) paths in the database, use the `show bgp ipv4 unicast paths` or `show bgp ipv6 unicast paths` command respectively.

```
show bgp {ipv4 | ipv6} unicast paths [regular-expression]
```

**Syntax Description**

| regular-expression  | (Optional) Regular expression used to match the paths received. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bgp ipv6 unicast paths` command:

```
> show bgp ipv6 unicast paths
Address   Hash Refcount Metric Path
0x61322A78  0   2  0   6346 8664 786 i
0x6131C214  3   2  0   3748 1275 8319 1273 209 i
0x6131D600 13   1  0   3748 1275 8319 12853 i
0x613229F0 17   1  1   4554 3748 4697 5408 i
0x61326818 32   1  1   4554 5609 i
0x61324AE0 34   1  0   6346 8664 9009 i
0x61323804 35   1  0   3748 1275 8319 i
0x61327918 35   1  0   237 2839 8664 i
0x61320504 38   2  0   3748 4697 1752 i
0x61320988 41   2  0   1849 786 i
0x6132245C 46   1  0   6346 8664 4927 i
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Internal address where the path is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Number of routes using that path.</td>
</tr>
<tr>
<td>Metric</td>
<td>The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td>
</tr>
<tr>
<td>Path</td>
<td>The autonomous system path for that route, followed by the origin code for that route.</td>
</tr>
</tbody>
</table>
show bgp ipv4/ ipv6 unicast prefix-list

To display routes that match a prefix list, use the `show bgp ipv4 prefix-list` or `show bgp ipv6 prefix-list` command.

```
show bgp {ipv4 | ipv6} unicast prefix-list name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-list name</td>
<td>The specified prefix-list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

The ipv6 prefix-list match the following prefixes:

```
  seq 5: matches the exact match 747::/16
  seq 10: first 32 bits in prefix must match with a prefixlen of /64
  seq 15: first 32 bits in prefix must match with any prefixlen up to /128
  seq 20: first 16 bits in prefix must match with any prefixlen up to /124
```
show bgp ipv4/ ipv6 unicast regexp

To display IPv4 or IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression, use the `show bgp ipv4 regexp` or `show bgp ipv6 regexp` command.

```
show bgp {ipv4 | ipv6} unicast regexp regular-expression
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>regexp</code></td>
<td>Regular expression that is used to match the BGP autonomous system paths</td>
</tr>
<tr>
<td><code>regular-expression</code></td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bgp ipv6 unicast regexp` command that shows paths beginning with 33 or containing 293. For an explanation of the output, see the `show bgp` command.

```
> show bgp ipv6 unicast regexp ^33|293
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
* 2001:200::/35 3FFE:C00:E:4::2 1 0 4554 293 3425 2500 i
* 2001:0DB8:0:F004::1 0 3320 293 3425 2500 i
* 2001:208::/35 3FFE:C00:E:4::2 1 0 4554 293 7610 i
* 2001:228::/35 3FFE:C00:E:F::2 0 6389 1849 293 7610 i
* 3FFE::/24 3FFE:C00:E:5::2 0 33 1849 293 1717 i
* 3FFE:100::/24 3FFE:C00:E:5::2 0 33 1849 3263 i
* 3FFE:300::/24 3FFE:C00:E:5::2 0 33 293 1275 1717 i
* 3FFE:C00:E:F::2 0 6389 1849 293 1275 i
```
show bgp ipv4/ipv6 unicast route-map

To display IPv4 or IPv6 Border Gateway Protocol (BGP) routes that failed to install in the routing table, use the `show bgp ipv4 unicast route-map` or `show bgp ipv6 unicast route-map` command.

```
show bgp {ipv4 | ipv6} unicast route-map name
```

**Syntax Description**

- `route-map name`: A specified route map to match.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bgp ipv6 unicast route-map` command for a route map named `rmap`. For an explanation of the output, see the `show bgp` command.

```
> show bgp ipv6 unicast route-map rmap
BGP table version is 16, local router ID is 172.30.242.1
Status codes: s suppressed, h history, * valid, > best, i - internal, r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network     Next Hop    Metric  LocPrf  Weight  Path
*112:12::/64 2001:0DB8:101::1 0 100   50   ?
*112:13::/64 2001:0DB8:101::1 0 100   50   ?
*112:14::/64 2001:0DB8:101::1 0 100   50   ?
*1543::/64   2001:0DB8:101::1 0 100   50   ?
```
show bgp ipv4/ ipv6 unicast summary

To display the status of all IPv4 or IPv6 Border Gateway Protocol (BGP) connections, use the `show bgp ipv4 unicast summary` or `show bgp ipv6 unicast summary` command respectively.

```bash
show bgp {ipv4 | ipv6} unicast summary
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show bgp ipv6 unicast summary` command:

```bash
> show bgp ipv6 unicast summary
BGP device identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
Neighbor  V  AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
2001:0DB8:101::2  4  200  6869  6882  0  0  0  06:25:24  Active
```

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

**Table 8: show bgp ipv4/ ipv6 unicast summary fields**

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

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the show bgp neighbors command.

```
show bgp neighbors [slow | ip-address | advertised-routes | paths [reg-exp] | policy [detail] |
                   received prefix-filter | received-routes | routes ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slow</td>
<td>(Optional) Displays information about dynamically configured slow peers.</td>
</tr>
<tr>
<td>ip-address</td>
<td>(Optional) Displays information about the IPv4 neighbor. If this argument is</td>
</tr>
<tr>
<td></td>
<td>omitted, information about all neighbors is displayed.</td>
</tr>
<tr>
<td>advertised-routes</td>
<td>(Optional) Displays all routes that have been advertised to neighbors.</td>
</tr>
<tr>
<td>paths [reg-exp]</td>
<td>(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.</td>
</tr>
<tr>
<td>policy</td>
<td>(Optional) Displays the policies applied to this neighbor per address family.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and autonomous system path filter lists.</td>
</tr>
<tr>
<td>received prefix-filter</td>
<td>(Optional) Displays the prefix-list (outbound route filter [ORF]) sent from the specified neighbor.</td>
</tr>
<tr>
<td>received-routes</td>
<td>(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.</td>
</tr>
<tr>
<td>routes</td>
<td>(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the received-routes keyword.</td>
</tr>
</tbody>
</table>

### Command Default

The output of this command displays information for all neighbors.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `show 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.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.
Examples

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```bash
> show bgp neighbors 10.108.50.2
BGP neighbor is 10.108.50.2, remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0

            Sent  Rcvd
  Opens:        3      3
  Notifications: 0      0
  Updates:      0      0
  Keepalives:   113    112
  Route Refresh: 0      0
  Total:        116    115

Default minimum time between advertisement runs is 5 seconds

For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member

                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

  Outbound  Inbound
  Local Policy Denied Prefixes: ------------  ------------
  Total:    0      0

Number of NLRIs in the update sent: max 0, min 0

  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
  External BGP neighbor may be up to 2 hops away.
  Connection state is ESTAB, I/O status: 1, unread input bytes: 0
  Connection is ECN Disabled
  Local host: 10.108.50.1, Local port: 179
  Foreign host: 10.108.50.2, Foreign port: 42698

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

  Event Timers (current time is 0x68B944):
  Timer        Starts  Wakeups  Next
Retrans 27 0 0x0
TimeWait 0 0 0x0
AckHold 27 18 0x0
SendWnd 0 0 0x0
KeepAlive 0 0 0x0
GiveUp 0 0 0x0
PmtuAger 0 0 0x0
DeadWait 0 0 0x0

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016  sndwnd: 15826
irs: 233567076  rcvnxt: 233567616  rcvwnd: 15845  delrcvwnd: 539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value: 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08

The following table describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are displayed only when the counter has a nonzero value.

Table 9: show bgp neighbors Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>IP address of the BGP neighbor and its autonomous system number.</td>
</tr>
<tr>
<td>remote AS</td>
<td>Autonomous system number of the neighbor.</td>
</tr>
<tr>
<td>local AS 300 no-prepend (not shown in display)</td>
<td>Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when migrating autonomous systems.</td>
</tr>
<tr>
<td>internal link</td>
<td>&quot;internal link&quot; is displayed for iBGP neighbors. &quot;external link&quot; is displayed for external BGP (eBGP) neighbors.</td>
</tr>
<tr>
<td>BGP version</td>
<td>BGP version being used to communicate with the remote router.</td>
</tr>
<tr>
<td>remote router ID</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>BGP state</td>
<td>Finite state machine (FSM) stage of session negotiation.</td>
</tr>
<tr>
<td>up for</td>
<td>Time, in hhmmss, that the underlying TCP connection has been in existence.</td>
</tr>
<tr>
<td>Last read</td>
<td>Time, in hhmmss, since BGP last received a message from this neighbor.</td>
</tr>
<tr>
<td>last write</td>
<td>Time, in hhmmss, since BGP last sent a message to this neighbor.</td>
</tr>
<tr>
<td>hold time</td>
<td>Time, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.</td>
</tr>
<tr>
<td>keepalive interval</td>
<td>Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Neighbor capabilities</td>
<td>BGP capabilities advertised and received from this neighbor. “advertised and received” is displayed when a capability is successfully exchanged between two routers.</td>
</tr>
<tr>
<td>Route Refresh</td>
<td>Status of the route refresh capability.</td>
</tr>
<tr>
<td>Graceful Restart Capability</td>
<td>Status of the graceful restart capability.</td>
</tr>
<tr>
<td>Address family IPv4 Unicast</td>
<td>IP Version 4 unicast-specific properties of this neighbor.</td>
</tr>
<tr>
<td>Message statistics</td>
<td>Statistics organized by message type.</td>
</tr>
<tr>
<td>InQ depth is</td>
<td>Number of messages in the input queue.</td>
</tr>
<tr>
<td>OutQ depth is</td>
<td>Number of messages in the output queue.</td>
</tr>
<tr>
<td>Sent</td>
<td>Total number of transmitted messages.</td>
</tr>
<tr>
<td>Received</td>
<td>Total number of received messages.</td>
</tr>
<tr>
<td>Opens</td>
<td>Number of open messages sent and received.</td>
</tr>
<tr>
<td>notifications</td>
<td>Number of notification (error) messages sent and received.</td>
</tr>
<tr>
<td>Updates</td>
<td>Number of update messages sent and received.</td>
</tr>
<tr>
<td>Keepalives</td>
<td>Number of keepalive messages sent and received.</td>
</tr>
<tr>
<td>Route Refresh</td>
<td>Number of route refresh request messages sent and received.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of messages sent and received.</td>
</tr>
<tr>
<td>Default minimum time between...</td>
<td>Time, in seconds, between advertisement transmissions.</td>
</tr>
<tr>
<td>For address family:</td>
<td>Address family to which the following fields refer.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>neighbor version</td>
<td>Number used by the software to track prefixes that have been sent and those that need to be sent.</td>
</tr>
<tr>
<td>update-group</td>
<td>Number of update-group member for this address family.</td>
</tr>
<tr>
<td>Prefix activity</td>
<td>Prefix statistics for this address family.</td>
</tr>
<tr>
<td>Prefixes current</td>
<td>Number of prefixes accepted for this address family.</td>
</tr>
<tr>
<td>Prefixes total</td>
<td>Total number of received prefixes.</td>
</tr>
<tr>
<td>Implicit Withdraw</td>
<td>Number of times that a prefix has been withdrawn and readvertised.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Explicit Withdraw</td>
<td>Number of times that prefix has been withdrawn because it is no longer feasible.</td>
</tr>
<tr>
<td>Used as bestpath</td>
<td>Number of received prefixes installed as bestpaths.</td>
</tr>
<tr>
<td>Used as multipath</td>
<td>Number of received prefixes installed as multipaths.</td>
</tr>
<tr>
<td>* Saved (soft-reconfig)</td>
<td>Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.</td>
</tr>
<tr>
<td>* History paths</td>
<td>This field is displayed only if the counter has a nonzero value.</td>
</tr>
<tr>
<td>* Invalid paths</td>
<td>Number of invalid paths. This field is displayed only if the counter has a nonzero value.</td>
</tr>
<tr>
<td>Local Policy Denied</td>
<td>Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.</td>
</tr>
<tr>
<td>Prefixes</td>
<td></td>
</tr>
<tr>
<td>* route-map</td>
<td>Displays inbound and outbound route-map policy denials.</td>
</tr>
<tr>
<td>* filter-list</td>
<td>Displays inbound and outbound filter-list policy denials.</td>
</tr>
<tr>
<td>* prefix-list</td>
<td>Displays inbound and outbound prefix-list policy denials.</td>
</tr>
<tr>
<td>* AS_PATH too long</td>
<td>Displays outbound AS-path length policy denials.</td>
</tr>
<tr>
<td>* AS_PATH loop</td>
<td>Displays outbound AS-path loop policy denials.</td>
</tr>
<tr>
<td>* AS_PATH confed info</td>
<td>Displays outbound confederation policy denials.</td>
</tr>
<tr>
<td>* AS_PATH contains AS 0</td>
<td>Displays outbound denials of autonomous system (AS) 0.</td>
</tr>
<tr>
<td>* NEXT_HOP Martian</td>
<td>Displays outbound martian denials.</td>
</tr>
<tr>
<td>* NEXT_HOP non-local</td>
<td>Displays outbound non-local next-hop denials.</td>
</tr>
<tr>
<td>* NEXT_HOP is us</td>
<td>Displays outbound next-hop-self denials.</td>
</tr>
<tr>
<td>* CLUSTER_LIST loop</td>
<td>Displays outbound cluster-list loop denials.</td>
</tr>
<tr>
<td>* ORIGINATOR loop</td>
<td>Displays outbound denials of local originated routes.</td>
</tr>
<tr>
<td>* unsuppress-map</td>
<td>Displays inbound denials due to an unsuppress-map.</td>
</tr>
<tr>
<td>* advertise-map</td>
<td>Displays inbound denials due to an advertise-map.</td>
</tr>
<tr>
<td>* Well-known Community</td>
<td>Displays inbound denials of well-known communities.</td>
</tr>
<tr>
<td>* SOO loop</td>
<td>Displays inbound denials due to site-of-origin.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>* Bestpath from this peer</td>
<td>Displays inbound denials because the bestpath came from the local router.</td>
</tr>
<tr>
<td>* Suppressed due to dampening</td>
<td>Displays inbound denials because the neighbor or link is in a dampening state.</td>
</tr>
<tr>
<td>* Bestpath from iBGP peer</td>
<td>Deploys inbound denials because the bestpath came from an iBGP neighbor.</td>
</tr>
<tr>
<td>* Incorrect RIB for CE</td>
<td>Deploys inbound denials due to RIB errors for a CE router.</td>
</tr>
<tr>
<td>* BGP distribute-list</td>
<td>Displays inbound denials due to a distribute list.</td>
</tr>
<tr>
<td>Number of NLRIs...</td>
<td>Number of network layer reachability attributes in updates.</td>
</tr>
<tr>
<td>Connections established</td>
<td>Number of times a TCP and BGP connection has been successfully established.</td>
</tr>
<tr>
<td>dropped</td>
<td>Number of times that a valid session has failed or been taken down.</td>
</tr>
<tr>
<td>Last reset</td>
<td>Time since this peering session was last reset. The reason for the reset is displayed on this line.</td>
</tr>
<tr>
<td>External BGP neighbor may be... (not shown in the display)</td>
<td>Indicates that the BGP TTL security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.</td>
</tr>
<tr>
<td>Connection state</td>
<td>Connection status of the BGP peer.</td>
</tr>
<tr>
<td>Connection is ECN Disabled</td>
<td>Explicit congestion notification status (enabled or disabled).</td>
</tr>
<tr>
<td>Local host: 10.108.50.1, Local port: 179</td>
<td>IP address of the local BGP speaker. BGP port number 179.</td>
</tr>
<tr>
<td>Foreign host: 10.108.50.2, Foreign port: 42698</td>
<td>Neighbor address and BGP destination port number.</td>
</tr>
<tr>
<td>Enqueued packets for retransmit:</td>
<td>Packets queued for retransmission by TCP.</td>
</tr>
<tr>
<td>Event Timers</td>
<td>TCP event timers. Counters are provided for starts and wakeups (expired timers).</td>
</tr>
<tr>
<td>Retrans</td>
<td>Number of times a packet has been retransmitted.</td>
</tr>
<tr>
<td>TimeWait</td>
<td>Time waiting for the retransmission timers to expire.</td>
</tr>
<tr>
<td>AckHold</td>
<td>Acknowledgment hold timer.</td>
</tr>
<tr>
<td>SendWnd</td>
<td>Transmission (send) window.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>KeepAlive</td>
<td>Number of keepalive packets.</td>
</tr>
<tr>
<td>GiveUp</td>
<td>Number times a packet is dropped due to no acknowledgment.</td>
</tr>
<tr>
<td>PmtuAger</td>
<td>Path MTU discovery timer</td>
</tr>
<tr>
<td>DeadWait</td>
<td>Expiration timer for dead segments.</td>
</tr>
<tr>
<td>iss:</td>
<td>Initial packet transmission sequence number.</td>
</tr>
<tr>
<td>snduna</td>
<td>Last transmission sequence number that has not been acknowledged.</td>
</tr>
<tr>
<td>sndnxt:</td>
<td>Next packet sequence number to be transmitted.</td>
</tr>
<tr>
<td>sndwnd:</td>
<td>TCP window size of the remote neighbor.</td>
</tr>
<tr>
<td>irs:</td>
<td>Initial packet receive sequence number.</td>
</tr>
<tr>
<td>rcvnxt:</td>
<td>Last receive sequence number that has been locally acknowledged.</td>
</tr>
<tr>
<td>rcvwnd:</td>
<td>TCP window size of the local host.</td>
</tr>
<tr>
<td>delrcvwnd:</td>
<td>Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.</td>
</tr>
<tr>
<td>SRTT:</td>
<td>A calculated smoothed round-trip timeout.</td>
</tr>
<tr>
<td>RTTO:</td>
<td>Round-trip timeout.</td>
</tr>
<tr>
<td>RTV:</td>
<td>Variance of the round-trip time.</td>
</tr>
<tr>
<td>KRTT:</td>
<td>New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.</td>
</tr>
<tr>
<td>minRTT:</td>
<td>Smallest recorded round-trip timeout (hard-wire value used for calculation).</td>
</tr>
<tr>
<td>maxRTT:</td>
<td>Largest recorded round-trip timeout.</td>
</tr>
<tr>
<td>ACK hold:</td>
<td>Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.</td>
</tr>
<tr>
<td>IP Precedence value:</td>
<td>IP precedence of the BGP packets.</td>
</tr>
<tr>
<td>Datagrams</td>
<td>Number of update packets received from a neighbor.</td>
</tr>
<tr>
<td>Reqd:</td>
<td>Number of received packets.</td>
</tr>
<tr>
<td>with data</td>
<td>Number of update packets sent with data.</td>
</tr>
<tr>
<td>total data bytes</td>
<td>Total amount of data received, in bytes.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of update packets sent.</td>
</tr>
</tbody>
</table>
### Table 1: show bgp neighbors Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second Congestion</td>
<td>Number of second retransmissions sent due to congestion.</td>
</tr>
<tr>
<td>Datagrams: Rcvd</td>
<td>Number of update packets received from a neighbor.</td>
</tr>
<tr>
<td>out of order:</td>
<td>Number of packets received out of sequence.</td>
</tr>
<tr>
<td>with data</td>
<td>Number of update packets received with data.</td>
</tr>
<tr>
<td>Last reset</td>
<td>Elapsed time since this peering session was last reset.</td>
</tr>
<tr>
<td>unread input bytes</td>
<td>Number of bytes of packets still to be processed.</td>
</tr>
<tr>
<td>retransmit</td>
<td>Number of packets retransmitted.</td>
</tr>
<tr>
<td>fastretransmit</td>
<td>Number of duplicate acknowledgments retransmitted for an out of order segment before the retransmission timer expires.</td>
</tr>
<tr>
<td>partialack</td>
<td>Number of retransmissions for partial acknowledgments (transmissions before or without subsequent acknowledgments).</td>
</tr>
</tbody>
</table>

The following example displays routes advertised for only the 172.16.232.178 neighbor. For an explanation of the output, see the `show bgp` command.

```
> show bgp neighbors 172.16.232.178 advertised-routes
BGP table version is 27, local router ID is 172.16.232.181
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
*>10.0.0.0.0 172.16.232.179  0       100    0  ?
*> 10.20.2.0  10.0.0.0   0        32768  1
```

The following is example output from the `show bgp neighbors` command entered with the `paths` keyword:

```
> show bgp neighbors 172.29.232.178 paths ^10
Address   Refcount Metric Path
0x60E577B0 2     40 10  ?
```

The following table explains each field.

### Table 10: show bgp neighbors paths Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Internal address where the path is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Number of routes using that path.</td>
</tr>
<tr>
<td>Metric</td>
<td>Multi Exit Discriminator (MED) metric for the path.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system path for that route, followed by the origin code for that route.</td>
</tr>
</tbody>
</table>
The following example shows that a prefix-list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```bash
> show bgp neighbors 192.168.20.72 received prefix-filter
Address family: IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
  seq 5 deny 10.0.0.0/8 le 32
```

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays policies configured on the neighbor device.

```bash
> show bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:  
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  route-map ROUTE in
    weight 300
  maximum-prefix 10000
```

The following is sample output from the `show bgp neighbors` command that verifies that BGP TCP path maximum transmission unit (MTU) discovery is enabled for the BGP neighbor at 172.16.1.2:

```bash
> show bgp neighbors 172.16.1.2
BGP neighbor is 172.16.1.2, remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
  For address family: IPv4 Unicast
    BGP table version 5, neighbor version 5/0
    Address tracking is enabled, the RIB does have a route to 172.16.1.2
    Address tracking requires at least a /24 route to the peer
    Connections established 3; dropped 2
    Last reset 00:00:35, due to Router ID changed
    Transport(tcp) path-mtu-discovery is enabled
    SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
    minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
    Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```
show bgp paths

To display all the BGP paths in the database, use the `show bgp paths` command.

```
show bgp paths [regexp]
```

**Syntax Description**

| regexp       | Regular expression to match the BGP autonomous system paths. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bgp paths` command.

```
> show bgp paths
Address       Hash  Refcount Metric Path
0x60E5742C   0      1       0 1
0x60E3D7AC   2      1       0 ?
0x60E5C6C0   11     3       0 10 ?
0x60E577B0   35     2       40 10 ?
```

The following table explains each field.

**Table 11: show bgp paths Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Internal address where the path is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Hash bucket where path is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Number of routes using that path.</td>
</tr>
<tr>
<td>Metric</td>
<td>The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td>
</tr>
<tr>
<td>Path</td>
<td>The autonomous system path for that route, followed by the origin code for that route.</td>
</tr>
</tbody>
</table>
show bgp prefix-list

To display information about a prefix list or prefix list entries, use the `show bgp prefix-list` command.

```
show bgp prefix-list [ detail | summary ] [ prefix-list-name [ seq sequence-number | network/length [ longer | first-match ] ] ]
```

**Syntax Description**

- **detail** | **summary** 
  (Optional) Displays detailed or summarized information about all prefix lists.
- **first-match** 
  (Optional) Displays the first entry of the specified prefix list that matches the given network/length.
- **longer** 
  (Optional) Displays all entries of the specified prefix list that match or are more specific than the given network/length.
- **network/length** 
  (Optional) Displays all entries in the specified prefix list that use this network address and netmask length (in bits).
- **prefix-list-name** 
  (Optional) Displays the entries in a specific prefix list.
- **seq sequence-number** 
  (Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix-list.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the output of the `show bgp prefix-list` command with details about the prefix list named test:

```
> show bgp prefix-list detail test
ip prefix-list test:
Description: test-list
  count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
  seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```
show bgp regexp

To display routes matching the autonomous system path regular expression, use the `show bgp regexp` command.

```
show bgp regexp  regexp
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>regexp</td>
<td>Regular expression to match the BGP autonomous system paths.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bgp regexp` command.

```
> show bgp regexp 108$
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network  Next Hop   Metric LocPrf Weight Path
  * 172.16.0.0  172.16.72.30  0 109 108 ?
  * 172.16.1.0  172.16.72.30  0 109 108 ?
  * 172.16.11.0 172.16.72.30  0 109 108 ?
  * 172.16.14.0 172.16.72.30  0 109 108 ?
  * 172.16.15.0 172.16.72.30  0 109 108 ?
  * 172.16.16.0 172.16.72.30  0 109 108 ?
  * 172.16.17.0 172.16.72.30  0 109 108 ?
  * 172.16.18.0 172.16.72.30  0 109 108 ?
  * 172.16.19.0 172.16.72.30  0 109 108 ?
  * 172.16.24.0 172.16.72.30  0 109 108 ?
  * 172.16.29.0 172.16.72.30  0 109 108 ?
  * 172.16.30.0 172.16.72.30  0 109 108 ?
  * 172.16.33.0 172.16.72.30  0 109 108 ?
  * 172.16.35.0 172.16.72.30  0 109 108 ?
  * 172.16.36.0 172.16.72.30  0 109 108 ?
  * 172.16.37.0 172.16.72.30  0 109 108 ?
  * 172.16.38.0 172.16.72.30  0 109 108 ?
  * 172.16.39.0 172.16.72.30  0 109 108 ?
```
show bgp rib-failure

To display Border Gateway Protocol (BGP) routes that failed to install in the Routing Information Base (RIB) table, use the `show bgp rib-failure` command.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following is a sample output from the `show bgp rib-failure` command:

```
> show bgp rib-failure
Network   Next Hop       RIB-failure               RIB-NH Matches
10.1.15.0/24 10.1.35.5  Higher admin distance  n/a
10.1.16.0/24 10.1.15.1  Higher admin distance  n/a
```

The following table explains each field.

**Table 12: show bgp rib-failure Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>IP address of a network entity</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.</td>
</tr>
<tr>
<td>RIB-failure</td>
<td>Cause of RIB failure. Higher admin distance means that a route with a better (lower) administrative distance such as a static route already exists in the IP routing table.</td>
</tr>
<tr>
<td>RIB-NH Matches</td>
<td>Route status that applies only when Higher admin distance appears in the RIB-failure column and <code>bgp suppress-inactive</code> is configured for the address family being used. There are three choices:</td>
</tr>
<tr>
<td></td>
<td>• Yes—Means that the route in the RIB has the same next hop as the BGP route or next hop recurses down to the same adjacency as the BGP nexthop.</td>
</tr>
<tr>
<td></td>
<td>• No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route.</td>
</tr>
<tr>
<td></td>
<td>• n/a—Means that <code>bgp suppress-inactive</code> is not configured for the address family being used.</td>
</tr>
</tbody>
</table>
show bgp summary

To display the status of all Border Gateway Protocol (BGP) connections, use the **show bgp summary** command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **show bgp summary** command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route. A path is a route to a given destination. By default, BGP will install only a single path for each destination. If multipath routes are configured, BGP will install a path entry for each multipath route, and only one multipath route will be marked as the best path.

BGP attribute and cache entries are displayed individually and in combinations that affect the bestpath selection process. The fields for this output are displayed when the related BGP feature is configured or attribute is received. Memory usage is displayed in bytes.

### Examples

The following is sample output from the **show bgp summary** command in privileged EXEC mode:

```plaintext
> show bgp summary
BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs
Neighbor    V  AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.100.1.1   4  200  26  22  199 0 0 00:14:23 23
10.200.1.1   4  300  21  51  199 0 0 00:13:40 0
```

The following table explains each field.
Table 13: show bgp summary Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP router identifier</td>
<td>In order of precedence and availability, the router identifier, a loopback address, or the highest IP address.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Internal version number of BGP database.</td>
</tr>
<tr>
<td>main routing table version</td>
<td>Last version of BGP database that was injected into the main routing table.</td>
</tr>
<tr>
<td>...network entries</td>
<td>Number of unique prefix entries in the BGP database.</td>
</tr>
<tr>
<td>...using ... bytes of memory</td>
<td>Amount of memory, in bytes, that is consumed for the path, prefix, or attribute entry displayed on the same line.</td>
</tr>
<tr>
<td>...path entries using</td>
<td>Number of path entries in the BGP database. Only a single path entry will be installed for a given destination. If multipath routes are configured, a path entry will be installed for each multipath route.</td>
</tr>
<tr>
<td>...multipath network entries using</td>
<td>Number of multipath entries installed for a given destination.</td>
</tr>
<tr>
<td>* ...BGP path/bestpath attribute entries using</td>
<td>Number of unique BGP attribute combinations for which a path is selected as the bestpath.</td>
</tr>
<tr>
<td>* ...BGP rinfo entries using</td>
<td>Number of unique ORIGINATOR and CLUSTER_LIST attribute combinations.</td>
</tr>
<tr>
<td>...BGP AS-PATH entries using</td>
<td>Number of unique AS_PATH entries.</td>
</tr>
<tr>
<td>...BGP community entries using</td>
<td>Number of unique BGP community attribute combinations.</td>
</tr>
<tr>
<td>*...BGP extended community entries using</td>
<td>Number of unique extended community attribute combinations.</td>
</tr>
<tr>
<td>BGP route-map cache entries using</td>
<td>Number of BGP route-map match and set clause combinations. A value of 0 indicates that the route cache is empty.</td>
</tr>
<tr>
<td>...BGP filter-list cache entries using</td>
<td>Number of filter-list entries that match an AS-path access list permit or deny statements. A value of 0 indicates that the filter-list cache is empty.</td>
</tr>
<tr>
<td>BGP advertise-bit cache entries using</td>
<td>Number of advertised bitfield entries and the associated memory usage. A bitfield entry represents a piece of information (one bit) that is generated when a prefix is advertised to a peer. The advertised bit cache is built dynamically when required</td>
</tr>
<tr>
<td>...received paths for inbound soft reconfiguration</td>
<td>Number paths received and stored for inbound soft reconfiguration.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BGP using...</td>
<td>Total amount of memory, in bytes, used by the BGP process.</td>
</tr>
<tr>
<td>Dampening enabled...</td>
<td>Indicates that BGP dampening is enabled. The number of paths that carry an accumulated penalty and the number of dampened paths are displayed on this line.</td>
</tr>
<tr>
<td>BGP activity...</td>
<td>Displays the number of times that memory has been allocated or released for a path or prefix.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>V</td>
<td>BGP version number spoken to the neighbor.</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous system number.</td>
</tr>
<tr>
<td>MsgRcvd</td>
<td>Number of messages received from the neighbor.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>Number of messages sent to the neighbor.</td>
</tr>
<tr>
<td>TblVer</td>
<td>Last version of the BGP database that was sent to the neighbor.</td>
</tr>
<tr>
<td>InQ</td>
<td>Number of messages queued to be processed from the neighbor.</td>
</tr>
<tr>
<td>OutQ</td>
<td>Number of messages queued to be sent to the neighbor.</td>
</tr>
<tr>
<td>Up/Down</td>
<td>The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.</td>
</tr>
<tr>
<td>State/PfxRcd</td>
<td>Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number is reached, the string &quot;PfxRcd&quot; appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down.</td>
</tr>
</tbody>
</table>

The following output from the `show bgp summary` command shows that the BGP neighbor 192.168.3.2 was dynamically created and is a member of the listen range group, group192. The output also shows that the IP prefix range of 192.168.0.0/16 is defined for the listen range group named group192.

```bash
> show bgp summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
   *192.168.3.2 4 50000 2 2 0 0 0 00:00:37 0
   * Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
   192.168.0.0/16
```

The following output from the `show bgp summary` command shows two BGP neighbors, 192.168.1.2 and 192.168.3.2, in different 4-byte autonomous system numbers, 65536 and 65550. The local
autonomous system 65538 is also a 4-byte autonomous system number and the numbers are displayed in the default asplain format.

```shell
> show bgp summary
BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor   V  AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down Statd
192.168.1.2 4  65536    7    7   1   0   0 00:03:04  0
192.168.3.2 4  65550    4    4   1   0   0 00:00:15  0
```

The following output from the `show bgp summary` command shows the same two BGP neighbors, but the 4-byte autonomous system numbers are displayed in asdot notation format.

```shell
> show bgp summary
BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor   V  AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down Statd
192.168.1.2 4  1.0    9    9   1   0   0 00:04:13  0
192.168.3.2 4  1.14   6    6   1   0   0 00:01:24  0
```
show bgp update-group

To display information about BGP update-groups, use the `show bgp update-group` command.

```
show bgp update-group [index-group | ip-address] [summary]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>index-group</td>
<td>(Optional) Update group type with its corresponding index number. The range of update-group index numbers is from 1 to 4294967295.</td>
</tr>
<tr>
<td>ip-address</td>
<td>(Optional) IP address of a single neighbor who is a member of an update group.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays a summary of update-group member information. The output can be filtered to show information for a single index group or peer with the index-group or ip-address argument.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

| Usage Guidelines   |                                                  |
|--------------------|                                                  |
|                    | Use this command to display information about BGP update groups. When a change to BGP outbound policy occurs, the router automatically recalculates update group memberships and applies the changes by triggering an outbound soft reset after a 1-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration if a mistake is made. |

Examples

The following sample output from the `show bgp update-group` command shows update group information for all neighbors:

```
> show bgp update-group
BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Route map for outgoing advertisements is COST1
  Update messages formatted 0, replicated 0
  Number of NLRI's in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 1 member:
    10.4.9.21
BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Update messages formatted 0, replicated 0
  Number of NLRI's in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 2 members:
    10.4.9.5 10.4.9.8
```

The following table explains each field.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP version</td>
<td>BGP version.</td>
</tr>
<tr>
<td>update-group</td>
<td>Update-group number and type (internal or external).</td>
</tr>
<tr>
<td>update messages formatted...</td>
<td>Number of update messages that have been formatted and replicated.</td>
</tr>
<tr>
<td>Number of NLRIs...</td>
<td>NLRI information sent in update.</td>
</tr>
<tr>
<td>Minimum time between...</td>
<td>Amount of memory, in bytes, that is consumed for the path, prefix, or attribute entry displayed on the same line.</td>
</tr>
<tr>
<td>...path entries using</td>
<td>Number of path entries in the BGP database. Only a single path entry will be installed for a given destination. If multipath routes are configured, a path entry will be installed for each multipath route.</td>
</tr>
<tr>
<td>...multipath network entries using</td>
<td>Number of multipath entries installed for a given destination.</td>
</tr>
<tr>
<td>* ...BGP path/bestpath attribute entries using</td>
<td>Number of unique BGP attribute combinations for which a path is selected as the bestpath.</td>
</tr>
<tr>
<td>* ...BGP rinfo entries using</td>
<td>Number of unique ORIGINATOR and CLUSTER_LIST attribute combinations.</td>
</tr>
<tr>
<td>...BGP AS-PATH entries using</td>
<td>Number of unique AS_PATH entries.</td>
</tr>
<tr>
<td>...BGP community entries using</td>
<td>Number of unique BGP community attribute combinations.</td>
</tr>
<tr>
<td>*...BGP extended community entries using</td>
<td>Number of unique extended community attribute combinations.</td>
</tr>
<tr>
<td>BGP route-map cache entries using</td>
<td>Number of BGP route-map match and set clause combinations. A value of 0 indicates that the route cache is empty.</td>
</tr>
<tr>
<td>...BGP filter-list cache entries using</td>
<td>Number of filter-list entries that match an AS-path access list permit or deny statements. A value of 0 indicates that the filter-list cache is empty.</td>
</tr>
<tr>
<td>BGP advertise-bit cache entries using</td>
<td>Number of advertised bitfield entries and the associated memory usage. A bitfield entry represents a piece of information (one bit) that is generated when a prefix is advertised to a peer. The advertised bit cache is built dynamically when required</td>
</tr>
<tr>
<td>...received paths for inbound soft reconfiguration</td>
<td>Number paths received and stored for inbound soft reconfiguration.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BGP using...</td>
<td>Total amount of memory, in bytes, used by the BGP process.</td>
</tr>
<tr>
<td>Dampening enabled...</td>
<td>Indicates that BGP dampening is enabled. The number of paths that carry an accumulated penalty and the number of dampened paths are displayed on this line.</td>
</tr>
<tr>
<td>BGP activity...</td>
<td>Displays the number of times that memory has been allocated or released for a path or prefix.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>V</td>
<td>BGP version number spoken to the neighbor.</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous system number.</td>
</tr>
<tr>
<td>MsgRcvd</td>
<td>Number of messages received from the neighbor.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>Number of messages sent to the neighbor.</td>
</tr>
<tr>
<td>TblVer</td>
<td>Last version of the BGP database that was sent to the neighbor.</td>
</tr>
<tr>
<td>InQ</td>
<td>Number of messages queued to be processed from the neighbor.</td>
</tr>
<tr>
<td>OutQ</td>
<td>Number of messages queued to be sent to the neighbor.</td>
</tr>
<tr>
<td>Up/Down</td>
<td>The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.</td>
</tr>
<tr>
<td>State/PfxRcd</td>
<td>Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number is reached, the string &quot;PfxRcd&quot; appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down.</td>
</tr>
</tbody>
</table>
# show blocks

To show the system buffer utilization, use the `show blocks` command.

```plaintext
show blocks [core | export-failed | interface]
show blocks address hex [diagnostics | dump | header | packet]
show blocks {all | assigned | free | old} [core-local [core-num] [diagnostics | dump | header | packet]]
show blocks exhaustion {history [list | snapshot_num] | snapshot}
show blocks pool block-size
show blocks queue history [core-local [core-num]] [detail]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address hex</td>
<td>(Optional) Shows a block corresponding to this address, in hexadecimal.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Shows all blocks.</td>
</tr>
<tr>
<td>assigned</td>
<td>(Optional) Shows blocks that are assigned and in use by an application.</td>
</tr>
<tr>
<td>core</td>
<td>(Optional) Shows core-specific buffers.</td>
</tr>
<tr>
<td>core-local [core-num]</td>
<td>(Optional) Shows system buffers for all cores. You can also specify a core</td>
</tr>
<tr>
<td></td>
<td>number, for example, 1, to see the buffers for a specific core.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Shows a portion (128 bytes) of the first block for each unique</td>
</tr>
<tr>
<td></td>
<td>queue type.</td>
</tr>
<tr>
<td>dump</td>
<td>(Optional) Shows the entire block contents, including the header and packet</td>
</tr>
<tr>
<td></td>
<td>information. The difference between dump and packet is that dump includes</td>
</tr>
<tr>
<td></td>
<td>additional information between the header and the packet.</td>
</tr>
<tr>
<td>diagnostics</td>
<td>(Optional) Shows block diagnostics.</td>
</tr>
<tr>
<td>exhaustion snapshot</td>
<td>(Optional) Prints the last x number (x is currently 10) of snapshots that</td>
</tr>
<tr>
<td></td>
<td>were taken and the time stamp of the last snapshot). After a snapshot is</td>
</tr>
<tr>
<td></td>
<td>taken, another snapshot is not taken if less than 5 minutes has passed.</td>
</tr>
<tr>
<td>exhaustion history [list</td>
<td>snapshot_num]</td>
</tr>
<tr>
<td></td>
<td>snapshot number to limit information to a single snapshot, or list to see a</td>
</tr>
<tr>
<td></td>
<td>list of snapshots.</td>
</tr>
<tr>
<td>export-failed</td>
<td>(Optional) Show system buffer export failure counters.</td>
</tr>
<tr>
<td>free</td>
<td>(Optional) Shows blocks that are available for use.</td>
</tr>
<tr>
<td>header</td>
<td>(Optional) Shows the header of the block.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Show buffers attached to interfaces.</td>
</tr>
<tr>
<td>old</td>
<td>(Optional) Shows blocks that were assigned more than a minute ago.</td>
</tr>
<tr>
<td>packet</td>
<td>(Optional) Shows the header of the block as well as the packet contents.</td>
</tr>
</tbody>
</table>
The `show blocks` command helps you determine if the Firepower Threat Defense device is overloaded. This command lists preallocated system buffer utilization. A full memory condition is not a problem as long as traffic is moving through the Firepower Threat Defense device. You can use the `show conn` command to see if traffic is moving. If traffic is not moving and the memory is full, there may be a problem. You can also view this information using SNMP.

### Examples

The following is sample output from the `show blocks` command.

```
> show blocks
SIZE     MAX     LOW     CNT
  0     1450    1450    1450
   4     100      99      99
 256    4148    4135    4142
 512    6274    6270    6272
 1024    100     100     100
 2048    104     104     104
 4096    100     100     100
 8192    100     100     100
16384    100     100     100
32768    16      16      16
65536
```

The following table explains each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIZE</td>
<td>Size, in bytes, of the block pool. Each size represents a particular type.</td>
</tr>
<tr>
<td>0</td>
<td>Used by dupb blocks.</td>
</tr>
<tr>
<td>4</td>
<td>Duplicates existing blocks in applications such as DNS, ISAKMP, URL filtering, uauth, TFTP, and TCP modules. Also, this sized block can be used normally by code to send packets to drivers, etc.</td>
</tr>
<tr>
<td>80</td>
<td>Used in TCP intercept to generate acknowledgment packets and for failover hello messages.</td>
</tr>
</tbody>
</table>

---

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

(Optional) Shows blocks of a specific size.

(Optional) Shows where blocks are assigned when the Firepower Threat Defense device runs out of blocks. Sometimes, a block is allocated from the pool but never assigned to a queue. In that case, the location is the code address that allocated the block.
A summary of the document's content:

- **256**: Used for Stateful Failover updates, syslog, and other TCP functions. These blocks are mainly used for Stateful Failover messages. The active Firepower Threat Defense device generates and sends packets to the standby Firepower Threat Defense device to update the translation and connection table. In bursty traffic, where high rates of connections are created or torn down, the number of available blocks might drop to 0. This situation indicates that one or more connections were not updated to the standby Firepower Threat Defense device. The Stateful Failover protocol catches the missing translation or connection the next time. If the CNT column for 256-byte blocks stays at or near 0 for extended periods of time, then the Firepower Threat Defense device is having trouble keeping the translation and connection tables synchronized because of the number of connections per second that the Firepower Threat Defense device is processing.

- **Syslog messages sent out from the Firepower Threat Defense device also use the 256-byte blocks, but they are generally not released in such quantity to cause a depletion of the 256-byte block pool. If the CNT column shows that the number of 256-byte blocks is near 0, ensure that you are not logging at Debugging (level 7) to the syslog server. This is indicated by the logging trap line in the Firepower Threat Defense configuration. We recommend that you set logging at Notification (level 5) or lower, unless you require additional information for debugging purposes.

- **1550**: Used to store Ethernet packets for processing through the Firepower Threat Defense device. When a packet enters an interface, it is placed on the input interface queue, passed up to the operating system, and placed in a block. The device determines whether the packet should be permitted or denied based on the security policy and processes the packet through to the output queue on the outbound interface. If the device is having trouble keeping up with the traffic load, the number of available blocks will hover close to 0 (as shown in the CNT column of the command output). When the CNT column is zero, the device attempts to allocate more blocks. The maximum can be greater than 8192 for 1550-byte blocks if you issue this command. If no more blocks are available, the device drops the packet.

- **2048**: Control or guided frames used for control updates.

- **16384**: Only used for the 64-bit, 66-MHz Gigabit Ethernet cards (i82543).

- **MAX**: Maximum number of blocks available for the specified byte block pool. The maximum number of blocks is carved out of memory at bootup. Typically, the maximum number of blocks does not change. The exception is for the 256- and 1550-byte blocks, where the device can dynamically create more when needed. The maximum can be greater than 8192 for 1550-byte blocks if you issue this command.

- **LOW**: Low-water mark. This number indicates the lowest number of this size blocks available since the device was powered up, or since the last clearing of the blocks (with the clear blocks command). A zero in the LOW column indicates a previous event where memory was full.

- **CNT**: Current number of blocks available for that specific size block pool. A zero in the CNT column means memory is full now.

The following is sample output from the `show blocks all` command:
> `show blocks all`
Class 0, size 4

<table>
<thead>
<tr>
<th>Block</th>
<th>allocd_by</th>
<th>freed_by</th>
<th>data size</th>
<th>alloccnt</th>
<th>dup_cnt</th>
<th>oper</th>
<th>location</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01799940</td>
<td>0x00000000</td>
<td>0x000101603</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>alloc</td>
<td>not_specified</td>
</tr>
<tr>
<td>0x01798e80</td>
<td>0x00000000</td>
<td>0x000101603</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>alloc</td>
<td>not_specified</td>
</tr>
<tr>
<td>0x017983c0</td>
<td>0x00000000</td>
<td>0x000101603</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>alloc</td>
<td>not_specified</td>
</tr>
</tbody>
</table>

... Found 1000 of 1000 blocks
Displaying 1000 of 1000 blocks

The following table explains each field.

**Table 16: show blocks all Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>The block address.</td>
</tr>
<tr>
<td>allocd_by</td>
<td>The program address of the application that last used the block (0 if not used).</td>
</tr>
<tr>
<td>freed_by</td>
<td>The program address of the application that last released the block.</td>
</tr>
<tr>
<td>data size</td>
<td>The size of the application buffer/packet data that is inside the block.</td>
</tr>
<tr>
<td>allocnt</td>
<td>The number of times this block has been used since the block came into existence.</td>
</tr>
<tr>
<td>dup_cnt</td>
<td>The current number of references to this block if used: 0 means 1 reference, 1 means 2 references.</td>
</tr>
<tr>
<td>oper</td>
<td>One of the four operations that was last performed on the block: alloc, get, put, or free.</td>
</tr>
<tr>
<td>location</td>
<td>The application that uses the block, or the program address of the application that last allocated the block (same as the allocd_by field).</td>
</tr>
</tbody>
</table>

The following is sample output from the `show blocks exhaustion history list` command:

> `show blocks exhaustion history list`
1 Snapshot created at 18:01:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

2 Snapshot created at 18:02:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

3 Snapshot created at 18:03:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

4 Snapshot created at 18:04:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blocks</td>
<td>Increases the memory assigned to block diagnostics</td>
</tr>
<tr>
<td>clear blocks</td>
<td>Clears the system buffer statistics.</td>
</tr>
<tr>
<td>show conn</td>
<td>Shows active connections.</td>
</tr>
</tbody>
</table>
show bootvar

To show the boot file and configuration properties, use the `show bootvar` command.

```
show bootvar
```

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The BOOT variable specifies a list of bootable images on various devices. The CONFIG_FILE variable specifies the configuration file used during system initialization.

The output of this command is probably not meaningful for Firepower Threat Defense.

**Examples**

Following is an example of showing the boot variables for Firepower Threat Defense. Although the variables are empty, this example is from a functioning system.

```
> show bootvar
BOOT variable =
Current BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
```
show bridge-group

To show bridge group information such as interfaces assigned, MAC addresses, and IP addresses, use the `show bridge-group` command.

```
show bridge-group [bridge_group_number]
```

**Syntax Description**

- `bridge_group_number` Specifies the bridge group number as an integer between 1 and 250. If you do not specify a number, all bridge groups are shown.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was added.</td>
</tr>
<tr>
<td>6.2</td>
<td>We added support in routed firewall mode when using Integrated Routing and Bridging.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show bridge-group` command.

```
> show bridge-group
Static mac-address entries: 0 (in use), 16384 (max)
Dynamic mac-address entries: 0 (in use), 16384 (max)
Bridge Group: 1
Interfaces:
  GigabitEthernet1/2
  GigabitEthernet1/3
  GigabitEthernet1/4
  GigabitEthernet1/5
  GigabitEthernet1/6
  GigabitEthernet1/7
  GigabitEthernet1/8
Management System IP Address: 192.168.1.1 255.255.255.0
Management Current IP Address: 192.168.1.1 255.255.255.0
Management IPv6 Global Unicast Address(es):
  2000:100::1, subnet is 2000:100::/64
Static mac-address entries: 0
Dynamic mac-address entries: 0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Shows the bridge group interface configuration.</td>
</tr>
<tr>
<td>interface bvi</td>
<td></td>
</tr>
</tbody>
</table>
show bridge-group
show c

- show capture, on page 417
- show checkheaps, on page 420
- show checksum, on page 421
- show chunkstat, on page 422
- show clns, on page 423
- show cluster, on page 430
- show cluster info, on page 432
- show cluster rule hits, on page 436
- show community-list, on page 437
- show conn, on page 438
- show console-output, on page 447
- show coredump, on page 448
- show counters, on page 449
- show cpu, on page 451
- show crashinfo, on page 455
- show crypto accelerator load-balance, on page 457
- show crypto accelerator statistics, on page 459
- show crypto ca certificates, on page 465
- show crypto ca crls, on page 466
- show crypto ca trustpoints, on page 467
- show crypto ca trustpool, on page 468
- show crypto debug-condition, on page 470
- show crypto ikev1, on page 471
- show crypto ikev2, on page 473
- show crypto ipsec df-bit, on page 476
- show crypto ipsec fragmentation, on page 477
- show crypto ipsec policy, on page 478
- show crypto ipsec sa, on page 479
- show crypto ipsec stats, on page 486
- show crypto isakmp, on page 488
- show crypto key mypubkey, on page 491
- show crypto protocol statistics, on page 492
- show crypto sockets, on page 494
• show crypto ssl, on page 495
• show ctique, on page 498
• show ctl-provider, on page 500
• show curpriv, on page 501
show capture

To display the capture configuration when no options are specified, use the `show capture` command.

```
show capture [capture_name] [access-list access_list_name] [count number] [decode] [detail] [dump] [packet-number number] [trace]
```

**Syntax Description**

- `access-list access_list_name` (Optional) Displays information for packets that are based on IP or higher fields for the specific access list identification.
- `capture_name` (Optional) Specifies the name of the packet capture.
- `count number` (Optional) Displays the number of packets specified data. Valid values are from 0-4294967295.
- `decode` This option is useful when a capture of type isakmp is applied to an interface. All ISAKMP data flowing through that interface will be captured after decryption and shown with more information after decoding the fields.
- `detail` (Optional) Displays additional protocol information for each packet.
- `dump` (Optional) Displays a hexadecimal dump of the packets that are transported over the data link.
- `packet-number number` (Optional) Starts the display at the specified packet number. Valid values are from 0-4294967295.
- `trace` (Optional) Displays extended trace information for each packet - used if capture is set using the trace keyword as mentioned above, this will show the output of packet tracer for each packet in the inbound direction.

**Command History**

**Release** | **Modification**
---|---
6.1 | This command was introduced.

**Usage Guidelines**

If you specify the capture name, then the capture buffer contents for that capture are displayed.

The `dump` keyword does not display MAC information in the hexadecimal dump.

The decoded output of the packets depend on the protocol of the packet. In the following table, the bracketed output is displayed when you specify the `detail` keyword.

**Table 17: Packet Capture Output Formats**

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Capture Output Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q</td>
<td><code>HH:MM:SS.ms [ether-hdr] VLAN-info encap-ether-packet</code></td>
</tr>
<tr>
<td>ARP</td>
<td><code>HH:MM:SS.ms [ether-hdr] arp-type arp-info</code></td>
</tr>
</tbody>
</table>
### Packet Type | Capture Output Format
---|---
IP/Other | HH:MM:SS.ms [ether-hdr] src-addr dest-addr: ip-protocol ip-length
Other | HH:MM:SS.ms ether-hdr: hex-dump

If the Firepower Threat Defense device receives packets with an incorrectly formatted TCP header and drops them because of the ASP drop reason invalid-tcp-hdr-length, the `show capture` command output on the interface where those packets are received does not show those packets.

**Note**

When the file size option is used:

- The `show capture [capture_name]` command shows the number of packets captured and skipped.
- The `show capture` command shows the captured data in KB and MB.

### Examples

This example shows how to display the capture configuration:

```plaintext
> show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

This example shows how to display the packets that are captured by an ARP capture:

```plaintext
> show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

The following example shows how to display the packets that are captured on a single unit in a clustering environment:

```plaintext
> show capture
capture 1 cluster type raw-data interface primary interface cluster [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```
The following example shows how to display the packets that are captured on all units in a clustering environment:

```bash
> cluster exec show capture
mycapture (LOCAL):----------------------------------------------------------
capture 1 type raw-data interface primary [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]

yourcapture:----------------------------------------------------------------
capture 1 type raw-data interface primary [Capturing - 191484 bytes]
capture 2 type raw-data interface cluster [Capturing - 532354 bytes]
```

The following example shows the packets that are captured when SGT plus Ethernet tagging has been enabled on an interface:

```bash
> show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
```

When SGT plus Ethernet tagging has been enabled on an interface, the interface can still receive tagged or untagged packets. The example shown is for tagged packets, which have INLINE-TAG 36 in the output. When the same interface receives untagged packets, the output remains unchanged (that is, no “INLINE-TAG 36” entry is included in the output).

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>capture</td>
<td>Enables packet capture capabilities for packet sniffing and network fault isolation.</td>
</tr>
<tr>
<td></td>
<td>clear capture</td>
<td>Clears the capture buffer.</td>
</tr>
<tr>
<td></td>
<td>copy capture</td>
<td>Copies a capture file to a server.</td>
</tr>
</tbody>
</table>
show checkheaps

To show the checkheaps statistics, use the `show checkheaps` command. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show checkheaps` command:

```
> show checkheaps
Checkheaps stats from buffer validation runs
---------------------------
Time elapsed since last run : 42 secs
Duration of last run : 0 millisecs
Number of buffers created : 8082
Number of buffers allocated : 7809
Number of buffers free : 274
Total memory in use : 43570344 bytes
Total memory in free buffers : 87000 bytes
Total number of runs : 310
```
show checksum

To display the configuration checksum, use the **show checksum** command.

```
show checksum
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **show checksum** command allows you to display four groups of hexadecimal numbers that act as a digital summary of the configuration contents. This checksum is calculated only when you store the configuration in flash memory.

If a dot (".") appears before the checksum in the **show running-config** or **show checksum** command output, the output indicates a normal configuration load or write mode indicator (when loading from or writing to the Firepower Threat Defense flash partition). The "." shows that the Firepower Threat Defense device is preoccupied with the operation but is not “hung up.” This message is similar to a “system processing, please wait” message.

### Examples

This example shows how to display the configuration or the checksum:

```
> show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```
show chunkstat

To display the chunk statistics, use the **show chunkstat** command.

**show chunkstat**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to display the chunk statistics:

```
> show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end @ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01ede348, end @ 01ede37c
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show counters</td>
<td>Displays the protocol stack counters.</td>
</tr>
<tr>
<td>show cpu</td>
<td>Displays the CPU utilization information.</td>
</tr>
</tbody>
</table>
To show Connectionless-mode Network Service (CLNS) information for IS-IS, use the `show clns` command.

```plaintext
show clns {filter-set [name] | interface [interface_name] | is-neighbors [interface_name] [detail] | neighbors [areas] [interface_name] [detail] | protocol [domain] | traffic}
```

### Syntax Description
- **filter-set [name]**: Shows CLNS filter sets. You can optionally specify the name of a filter set.
- **interface [interface_name]**: Shows CLNS interface status and configuration. You can optionally specify the name of an interface to focus the output.
- **is-neighbors [interface_name] [detail]**: Shows IS neighbor adjacencies. Neighbor entries are sorted according to the area in which they are located. You can optionally specify the name of an interface to focus the output. Specify `detail` to include the areas associated with the intermediate systems. Otherwise, a summary display is provided.
- **neighbors [areas] [interface_name] [detail]**: Displays end system (ES), intermediate system (IS), and multitopology Integrated Intermediate System-to-Intermediate System (M-ISIS) neighbors. You can optionally specify the name of an interface to focus the output.
  - Include the `areas` keyword to show CLNS multiarea adjacencies.
  - Specify `detail` to include the areas associated with the intermediate systems. Otherwise, a summary display is provided.
- **protocol [domain]**: Shows CLNS routing protocol process information. There will always be at least two routing processes, a Level 1 and a Level 2, and there can be more. You can optionally specify the name of a CLNS domain to focus the output.
- **traffic**: Lists the CLNS packets that this router has seen.

### Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples
The following example shows the CLNS filter sets defined in the running configuration, and displays them using the `show clns filter-set` command.

```plaintext
> show running-config clns
clns filter-set US-OR-NORDUNET permit 47.0005...
clns filter-set US-OR-NORDUNET permit 47.0023...
clns filter-set LOCAL permit 49.0003
> show clns filter-set
CLNS filter set US-OR-NORDUNET
  permit 47.0005...
  permit 47.0023...
```
CLNS filter set LOCAL
   permit 49.0003...

The following is sample output from the show clns interface command. The information under "Routing Protocol: IS-IS" displays information pertaining to Intermediate System-to-Intermediate System (IS-IS), including the Level 1 and Level 2 metrics, priorities, circuit IDs, and number of active Level 1 and Level 2 adjacencies.

```plaintext
> show clns interface
GigabitEthernet0/1 is up, line protocol is up
   Checksums enabled, MTU 1500
   ERPDUs enabled, min. interval 10 msec.
   DEC compatibility mode OFF for this interface
   Next ESH/ISH in 0 seconds
   Routing Protocol: IS-IS
      Circuit Type: level-1-2
      Interface number 0x0, local circuit ID 0x1
      Level-1 Metric: 10, Priority: 64, Circuit ID: c2.01
      DR ID: c2.01
      Level-1 IPv6 Metric: 10
      Number of active level-1 adjacencies: 3
      Level-2 Metric: 10, Priority: 64, Circuit ID: c2.01
      DR ID: c2.01
      Level-2 IPv6 Metric: 10
      Number of active level-2 adjacencies: 3
      Next IS-IS LAN Level-1 Hello in 1 seconds
      Next IS-IS LAN Level-2 Hello in 1 seconds
```

The following is sample output from the show clns neighbors command.

```plaintext
> show clns neighbors
System IdInterface SNPA State Holdtime Type Protocol
CSR7001 inside 000c.2921.ff44 Up 29 L1L2
CSR7002 inside 000c.2906.491c Up 27 L1L2
```

The following table explains the fields in the neighbors output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Id</td>
<td>The six-byte value that identifies a system in an area.</td>
</tr>
<tr>
<td>Interface</td>
<td>The name of the interface from which the system was learned.</td>
</tr>
<tr>
<td>SNPA</td>
<td>The Subnetwork Point of Attachment. This is the data-link address.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the ES, IS, or M-ISIS.</td>
</tr>
<tr>
<td></td>
<td>• Init—The system is an IS and it is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent.</td>
</tr>
<tr>
<td></td>
<td>• Up—The system believes the ES or IS is reachable.</td>
</tr>
<tr>
<td>Holdtime</td>
<td>The number of seconds before this adjacency entry times out.</td>
</tr>
</tbody>
</table>
### Type

- **ES**—An end-system adjacency either discovered via the ES-IS protocol or statically configured.
- **IS**—A router adjacency either discovered via the ES-IS protocol or statically configured.
- **M-ISIS**—A router adjacency discovered via the multitopology IS-IS protocol.
- **L1**—A router adjacency for Level 1 routing only.
- **L1L2**—A router adjacency for Level 1 and Level 2 routing.
- **L2**—A router adjacency for Level 2 only.

### Protocol

Protocol through which the adjacency was learned. Valid protocol sources are ES-IS, IS-IS, ISO IGRP, Static, DECnet, and M-ISIS.

The following is sample output from the `show clns neighbors detail` command.

```plaintext
> show clns neighbors detail
System Id Interface SNPA State Holdtime Type Protocol
CSR7001 inside 000c.2921.ff44 Up 26 L1L2
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
CSR7002 inside 000c.2906.491c Up 27 L1L2
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
```

The following is sample output from the `show clns is-neighbors` command.

```plaintext
> show clns is-neighbors
System Id Interface State Type Priority Circuit Id Format
CSR7001 inside Up L1L2 64/64 ciscoasa.01 Phase V
CSR7002 inside Up L1L2 64/64 ciscoasa.01 Phase V
```

The following table explains the columns in the is-neighbors output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Id</td>
<td>The identification value of the system.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface on which the router was discovered.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>State</td>
<td>The adjacency state. Up and Init are the states. For details, see the show clns neighbors description.</td>
</tr>
<tr>
<td>Type</td>
<td>The adjacency type: L1, L2, or L1L2. For details, see the show clns neighbors description.</td>
</tr>
<tr>
<td>Priority</td>
<td>The IS-IS priority that the respective neighbor is advertising. The highest priority neighbor is elected the designated IS-IS router for the interface.</td>
</tr>
<tr>
<td>Circuit Id</td>
<td>The neighbor’s idea of what the designated IS-IS router is for the interface.</td>
</tr>
<tr>
<td>Format</td>
<td>The format, which indicates if the neighbor is either a Phase V (OSI) adjacency or Phase IV (DECnet) adjacency.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show clns is-neighbors detail` command.

```
> show clns is-neighbors detail
System Id Interface State Type Priority Circuit Id Format
CSR7001 inside Up L1L2 64/64 ciscoasa.01 Phase V
    Area Address(es): 49.0001
    IP Address(es): 1.3.3.3*
    Uptime: 00:12:49
    NSF capable
    Interface name: inside
CSR7002 inside Up L1L2 64/64 ciscoasa.01 Phase V
    Area Address(es): 49.0001
    IP Address(es): 20.3.3.3*
    Uptime: 00:12:50
    NSF capable
    Interface name: inside
```

The following is sample output from the `show clns protocol` command.

```
> show clns protocol
IS-IS Router
    System Id: 0050.0500.5008.00 IS-Type: level-1-2
    Manual area address(es):
        49.0001
    Routing for area address(es):
        49.0001
    Interfaces supported by IS-IS:
        outside - IP
    Distribute:
        static (on by default)
    Distance for L2 CLNS routes: 110
    RRR level: none
    Generate narrow metrics: level-1-2
    Accept narrow metrics: level-1-2
    Generate wide metrics: none
    Accept wide metrics: none
```

The following is sample output from the `show clns traffic` command.

```
> show clns traffic
CLNS: Time since last clear: never
```
CLNS & ESIS Output: 0, Input: 8829
CLNS Local: 0, Forward: 0
CLNS Discards:
  Hdr Syntax: 0, Checksum: 0, Lifetime: 0, Output cngstn: 0
  No Route: 0, Discard Route: 0, Dst Unreachable 0, Encaps. Failed: 0
  NLP Unknown: 0, Not an IS: 0
CLNS Options: Packets 0, total 0, bad 0, GQOS 0, cngstn exprncd 0
CLNS Segments: Segmented: 0, Failed: 0
CLNS Broadcasts: sent: 0, rcvd: 0
Echos: Rcvd 0 requests, 0 replies
  Sent 0 requests, 0 replies
ESIS(sent/rcvd): ESHs: 0/0, ISHs: 0/0, RDs: 0/0, QCF: 0/0
Tunneling (sent/rcvd): IP: 0/0, IPv6: 0/0
ISO-IGRP: Queries (sent/rcvd): 0/0 Updates (sent/rcvd): 0/0
ISO-IGRP Syntax Errors: 0
IS-IS: Time since last clear: never
IS-IS: Level-1 Hellos (sent/rcvd): 1928/1287
IS-IS: Level-2 Hellos (sent/rcvd): 1918/1283
IS-IS: PTP Hellos (sent/rcvd): 0/0
IS-IS: Level-1 LSPs sourced (new/refresh): 7/13
IS-IS: Level-2 LSPs sourced (new/refresh): 7/14
IS-IS: Level-1 LSPs flooded (sent/rcvd): 97/2675
IS-IS: Level-2 LSPs flooded (sent/rcvd): 73/2628
IS-IS: LSP Retransmissions: 0
IS-IS: Level-1 CSNPs (sent/rcvd): 642/0
IS-IS: Level-2 CSNPs (sent/rcvd): 639/0
IS-IS: Level-1 PSNPs (sent/rcvd): 0/554
IS-IS: Level-2 PSNPs (sent/rcvd): 0/390
IS-IS: Level-1 DR Elections: 1
IS-IS: Level-2 DR Elections: 1
IS-IS: Level-1 SPF Calculations: 9
IS-IS: Level-2 SPF Calculations: 8
IS-IS: Level-1 Partial Route Calculations: 0
IS-IS: Level-2 Partial Route Calculations: 0
IS-IS: LSP checksum errors received: 0
IS-IS: Update process queue depth: 0/200
IS-IS: Update process packets dropped: 0

The following table explains the fields in the traffic output.

**Table 20: Fields in the Traffic Output**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLNS &amp; ESIS Output</td>
<td>The total number of packets that this router has sent.</td>
</tr>
<tr>
<td>Input</td>
<td>The total number of packets that this router has received.</td>
</tr>
<tr>
<td>CLNS Local</td>
<td>The number of packets that were generated by this router.</td>
</tr>
<tr>
<td>Forward</td>
<td>The number of packets that this router has forwarded.</td>
</tr>
<tr>
<td>CLNS Discards</td>
<td>The number of packets that CLNS has discarded, classified by the reason for the discard.</td>
</tr>
<tr>
<td>CLNS Options</td>
<td>The options seen in CLNS packets.</td>
</tr>
<tr>
<td>Fields</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CLNS Segments</td>
<td>The number of packets segmented and the number of failures that occurred because a packet could not be segmented.</td>
</tr>
<tr>
<td>CLNS Broadcasts</td>
<td>The number of CLNS broadcasts sent and received.</td>
</tr>
<tr>
<td>Echos</td>
<td>The number of echo request packets and echo reply packets received. The line following this field lists the number of echo request packets and echo reply packets sent.</td>
</tr>
<tr>
<td>ESIS (sent/rcvd)</td>
<td>The number of End System Hello (ESH), Intermediate System Hello (ISH), and redirects sent and received.</td>
</tr>
<tr>
<td>ISO IGRP</td>
<td>The number of ISO Interior Gateway Routing Protocol (IGRP) queries and updates sent and received.</td>
</tr>
<tr>
<td>Router Hellos</td>
<td>The number of ISO IGRP router hello packets sent and received.</td>
</tr>
<tr>
<td>IS-IS: Level-1 hellos (sent/rcvd)</td>
<td>The number of Level 1 IS-IS hello packets sent and received.</td>
</tr>
<tr>
<td>IS-IS: Level-2 hellos (sent/rcvd)</td>
<td>The number of Level 2 IS-IS hello packets sent and received.</td>
</tr>
<tr>
<td>IS-IS: PTP hellos (sent/rcvd)</td>
<td>The number of point-to-point IS-IS hello packets sent and received over serial links.</td>
</tr>
<tr>
<td>IS-IS: Level-1 LSPs (sent/rcvd)</td>
<td>The number of Level 1 link-state Protocol Data Unit (PDUs) sent and received.</td>
</tr>
<tr>
<td>IS-IS: Level-2 LSPs (sent/rcvd)</td>
<td>The number of Level 2 link-state PDUs sent and received.</td>
</tr>
<tr>
<td>IS-IS: Level-1 CSNPs (sent/rcvd)</td>
<td>The number of Level 1 Complete Sequence Number Packets (CSNP) sent and received.</td>
</tr>
<tr>
<td>IS-IS: Level-2 CSNPs (sent/rcvd)</td>
<td>The number of Level 2 CSNPs sent and received.</td>
</tr>
<tr>
<td>IS-IS: Level-1 PSNPs (sent/rcvd)</td>
<td>The number of Level 1 Partial Sequence Number Packets (PSNP) sent and received.</td>
</tr>
<tr>
<td>IS-IS: Level-2 PSNPs (sent/rcvd)</td>
<td>The number of Level 2 PSNPs sent and received.</td>
</tr>
<tr>
<td>IS-IS: Level-1 DR Elections</td>
<td>The number of times Level 1 designated router election occurred.</td>
</tr>
<tr>
<td>IS-IS: Level-2 DR Elections</td>
<td>The number of times Level 2 designated router election occurred.</td>
</tr>
<tr>
<td>IS-IS: Level-1 SPF Calculations</td>
<td>The number of times the Level 1 shortest-path-first (SPF) tree was computed.</td>
</tr>
</tbody>
</table>
### IS-IS: Level-2 SPF Calculations

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS-IS: Level-2 SPF</td>
<td>The number of times the Level 2 SPF tree was computed.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear clns</td>
<td>Clears CLNS-specific information.</td>
</tr>
</tbody>
</table>
show cluster

To view aggregated data for the entire cluster or other information, use the `show cluster` command.

```
show cluster [access-list [acl_name] | conn [count] | cpu [usage] | history | interface-mode
| memory | resource usage | rule hits [raw] | service-policy | traffic | xlate count]
```

### Syntax Description

- **access-list [acl_name]**: Shows hit counters for access policies. To see the counters for a specific ACL, enter the `acl_name`.
- **conn [count]**: Shows the aggregated count of in-use connections for all units. If you enter the `count` keyword, only the connection count is shown.
- **cpu [usage]**: Shows CPU usage information.
- **history**: Shows cluster switching history.
- **interface-mode**: Shows the cluster interface mode, either spanned or individual.
- **memory**: Shows system memory utilization and other information.
- **resource usage**: Shows system resources and usage.
- **rule hits [raw]**: Shows rule hit information for all evaluated rules of access control policies and prefilter policies. The `raw` keyword shows the data in .csv format.
- **service-policy**: Shows the MPF service policy statistics.
- **traffic**: Shows traffic statistics.
- **xlate count**: Shows current translation information.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>Added the <code>rule hits [raw]</code> keywords.</td>
</tr>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show cluster access-list` command:

```
> show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B, unit-C, unit-D
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B, unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0
(hitcnt=0, 0, 0, 0, 0) 0xfe4f4947
access-list 101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
```
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access-list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104) 0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0xa143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfe4a
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d

To display the aggregated count of in-use connections for all units, enter:

> show cluster conn count

Usage Summary In Cluster:*********************************************
200 in use (cluster-wide aggregated)
  cl2(LOCAL):*********************************************
    100 in use, 100 most used
  cl1:*********************************************
    100 in use, 100 most used

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cluster info</td>
<td>Shows cluster information.</td>
</tr>
</tbody>
</table>
show cluster info

To view cluster information, use the `show cluster info` command.

```
show cluster info [ auto-join | clients | conn-distribution | flow-mobility counters | goid
| options | health | incompatible-config | loadbalance | old-members | packet-distribution
| trace | [options] | transport { asp | cp } ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auto-join</code></td>
<td>Shows whether the cluster unit will automatically rejoin the cluster after a time delay and if the failure conditions (such as waiting for the license, chassis health check failure, and so on) are cleared. If the unit is permanently disabled, or if the unit is already in the cluster, then this command will not show any output.</td>
</tr>
<tr>
<td><code>clients</code></td>
<td>(Optional) Shows the version of register clients.</td>
</tr>
<tr>
<td><code>conn-distribution</code></td>
<td>(Optional) Shows the connection distribution in the cluster.</td>
</tr>
<tr>
<td><code>flow-mobility counters</code></td>
<td>(Optional) Shows EID movement and flow owner movement information.</td>
</tr>
<tr>
<td><code>goid [options]</code></td>
<td>(Optional) Shows the global object ID database. Options include:</td>
</tr>
<tr>
<td></td>
<td>- classmap</td>
</tr>
<tr>
<td></td>
<td>- conn-set</td>
</tr>
<tr>
<td></td>
<td>- hwidb</td>
</tr>
<tr>
<td></td>
<td>- idfw-domain</td>
</tr>
<tr>
<td></td>
<td>- idfw-group</td>
</tr>
<tr>
<td></td>
<td>- interface</td>
</tr>
<tr>
<td></td>
<td>- policymap</td>
</tr>
<tr>
<td></td>
<td>- virtual-context</td>
</tr>
<tr>
<td><code>health</code></td>
<td>(Optional) Shows health monitoring information.</td>
</tr>
<tr>
<td><code>incompatible-config</code></td>
<td>(Optional) Shows commands that are incompatible with clustering in the current running configuration. This command is useful before you enable clustering.</td>
</tr>
<tr>
<td><code>loadbalance</code></td>
<td>(Optional) Shows load balancing information.</td>
</tr>
<tr>
<td><code>old-members</code></td>
<td>(Optional) Shows former members of the cluster.</td>
</tr>
<tr>
<td><code>packet-distribution</code></td>
<td>(Optional) Shows packet distribution in the cluster.</td>
</tr>
</tbody>
</table>
trace [options] (Optional) Shows the clustering control module event trace. Options include:

- latest [number]—Displays the latest number events, where the number is from 1 to 2147483647. The default is to show all.

- level level—Filters events by level where the level is one of the following: all, critical, debug, informational, or warning.

- module module—Filters events by module where the module is one of the following: ccp, datapath, fsm, general, hc, license, rpc, or transport.

- time [{month day} [hh:mm:ss]}—Shows events before the specified time or date.

transport {asp | cp} (Optional) Show transport related statistics for the following:

- asp—Data plane transport statistics.

- cp—Control plane transport statistics.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Added the auto-join keyword.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you do not specify any options, the show cluster info command shows general cluster information including the cluster name and status, the cluster members, the member states, and so on.

Clear statistics using the clear cluster info command.

Examples

The following is sample output from the show cluster info command:

```
> show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
    ID : 0
    Site ID : 1
    Version : 9.5(1)
    Serial No.: P3000000025
    CCL IP : 10.0.0.3
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2011
    Last leave: N/A
  Other members in the cluster:
    Unit "D" in state SLAVE
      ID : 1
      Site ID : 1
      Version : 9.5(1)
      Serial No.: P3000000001
      CCL IP : 10.0.0.4
      CCL MAC : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
```
Unit "A" in state MASTER
ID : 2
Site ID : 2
Version : 9.5(1)
Serial No.: JAB0815R0JY
CCL IP : 10.0.0.1
CCL MAC : 000f.f775.541e
Last join : 19:13:20 UTC Sep 23 2011
Last leave: N/A

Unit "B" in state SLAVE
ID : 3
Site ID : 2
Version : 9.5(1)
Serial No.: P3000000191
CCL IP : 10.0.0.2
CCL MAC : 000b.fcf8.c61e
Last join : 19:13:50 UTC Sep 23 2011
Last leave: 19:13:36 UTC Sep 23 2011

The following is sample output from the show cluster info incompatible-config command:

```
> show cluster info incompatible-config
INFO: Clustering is not compatible with following commands which given a
user's confirmation upon enabling clustering, can be removed automatically
from running-config.
policy-map global_policy
class scansafe-http
  inspect scansafe http-map fail-close
policy-map global_policy
class scansafe-https
  inspect scansafe https-map fail-close
INFO: No manually-correctable incompatible configuration is found.
```

The following is sample output from the show cluster info trace command:

```
> show cluster info trace
Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at MASTER
```

The following is sample output from the show cluster info flow-mobility counters command:

```
> show cluster info flow-mobility counters
EID movement notification received : 0
EID movement notification processed : 0
Flow owner moving requested : 0
```

See the following outputs for the show cluster info auto-join command:

```
> show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
```
Quit reason: Chassis-blade health check failed.

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.

> show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

> show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cluster</td>
<td>Displays aggregated data for the entire cluster.</td>
</tr>
</tbody>
</table>
# show cluster rule hits

To display rule hit information for all evaluated rules of access control policies and prefilter policies, from all nodes of a cluster in an aggregated format, use the `show cluster rule hits` command.

```
show cluster rule hits [raw]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>raw</th>
<th>(Optional) Displays the rule hit information in .csv format.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Displays rule hit information for all the rules from all nodes of a cluster.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>The rule hit information covers only the access control rules and prefilter rules.</th>
</tr>
</thead>
</table>

## Examples

The following example displays rule hit information from each node of a cluster in a segregated format:

```
> show cluster rule hits

<table>
<thead>
<tr>
<th>RuleID</th>
<th>Hit Count</th>
<th>First Hit Time (UTC)</th>
<th>Last Hit Time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>268435264</td>
<td>1</td>
<td>06:54:44 Mar 8 2019</td>
<td>06:54:44 Mar 8 2019</td>
</tr>
<tr>
<td>268435265</td>
<td>1</td>
<td>06:54:58 Mar 8 2019</td>
<td>06:54:58 Mar 8 2019</td>
</tr>
<tr>
<td>268435270</td>
<td>1</td>
<td>06:54:53 Mar 8 2019</td>
<td>06:54:53 Mar 8 2019</td>
</tr>
<tr>
<td>268435271</td>
<td>1</td>
<td>06:55:01 Mar 8 2019</td>
<td>06:55:01 Mar 8 2019</td>
</tr>
<tr>
<td>268435261</td>
<td>1</td>
<td>06:55:19 Mar 8 2019</td>
<td>06:55:19 Mar 8 2019</td>
</tr>
</tbody>
</table>
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cluster exec show rule hits</code></td>
<td>Display rule hit information for all evaluated rules of access control policies and prefilter policies from each node of a cluster in a segregated format.</td>
</tr>
<tr>
<td><code>cluster exec clear rule hits</code></td>
<td>Clears rule hit information for all evaluated rules of access control policies and prefilter policies and reset them to zero, from all nodes in a cluster.</td>
</tr>
<tr>
<td><code>show rule hits</code></td>
<td>Displays the rule hit information for all evaluated rules of access control policies and prefilter policies.</td>
</tr>
<tr>
<td><code>clear rule hits</code></td>
<td>Clears the rule hit information for all evaluated rules of access control policies and prefilter policies and resets them to zero.</td>
</tr>
</tbody>
</table>
show community-list

To display routes that are permitted by a specific community list, use the `show community-list` command.

```
show community-list [community_list_name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>community_list_name</th>
<th>(Optional) Community list name.</th>
</tr>
</thead>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show community-list` command:

```
> show community-list

Named Community expanded list comm2
  permit 10
Named Community standard list excomm1
  permit internet 100 no-export no-advertise
```
show conn

To display the connection state for the designated connection type, use the `show conn` command. This command supports IPv4 and IPv6 addresses.

```
show conn [ count | [ all ] | [ detail ] | [ long ] | [ state state_type ] | [ flow-rule ] | [ inline-set ]
| [ protocol { tcp | udp | sctp } ] | [ address src_ip [- src_ip ] | [ netmask mask ] ] | [ port
src_port [- src_port ] ] | [ address dest_ip [- dest_ip ] | [ netmask mask ] ] | [ port dest_port [-
dest_port ] ] | [ state state_type ] | [ zone [ zone_name ] ]
```

### Syntax Description

- **address {src_ip | dest_ip}** (Optional) Displays connections with the specified source or destination IPv4 or IPv6 address. To specify a range, separate the IP addresses with a dash (-). For example, 10.1.1.1-10.1.1.5.

- **all** (Optional) Displays connections that are to the device or from the device, in addition to through-traffic connections.

- **count** (Optional) Displays the number of active connections.

- **detail** (Optional) Displays connections in detail, including translation type and interface information.

- **flow-rule** (Optional) Displays connections of a flow rule.

- **inline-set** (Optional) Displays connections of an inline-set.

- **long** (Optional) Displays connections in long format.

- **netmask mask** (Optional) Specifies a subnet mask for use with the given IP address.

- **port {src_port | dest_port}** (Optional) Displays connections with the specified source or destination port. To specify a range, separate the port numbers with a dash (-). For example, 1000-2000.

- **protocol {tcp | udp | sctp}** (Optional) Specifies the connection protocol.

- **state state_type** (Optional) Specifies the connection state type. See the table in the usage section for a list of the keywords available for connection state types.

- **zone [zone_name]** (Optional) Displays connections for a zone. The `long` and `detail` keywords show the primary interface on which the connection was built and the current interface used to forward the traffic.

### Command Default

All through connections are shown by default. You need to use the `all` keyword to also view management connections to the device.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>The egress_optimization connection state type was added.</td>
</tr>
<tr>
<td>6.5</td>
<td>Dead Connection Detection (DCD) initiator/responder probe counts were added to the show conn detail output for DCD-enabled connections.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The show conn command displays the number of active TCP and UDP connections, and provides information about connections of various types. Use the show conn all command to see the entire table of connections. You can use this command to find the live connections that are being rate limited by a specific QoS rule ID.

Usage Guidelines

When the Firepower Threat Defense device creates a pinhole to allow secondary connections, this is shown as an incomplete conn by the show conn command. To clear this incomplete conn use the clear conn command.

Usage Guidelines

The connection types that you can specify using the show conn state command are defined in the following table. When specifying multiple connection types, use commas without spaces to separate the keywords. The following example displays information about RPC, H.323, and SIP connections in the Up state:

> show conn state up, rpc, h323, sip

### Table 21: Connection State Types

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Connection Type Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>up</td>
<td>Connections in the up state.</td>
</tr>
<tr>
<td>conn_inbound</td>
<td>Inbound connections.</td>
</tr>
<tr>
<td>ctiqbe</td>
<td>CTIQBE connections</td>
</tr>
<tr>
<td>data_in</td>
<td>Inbound data connections.</td>
</tr>
<tr>
<td>data_out</td>
<td>Outbound data connections.</td>
</tr>
<tr>
<td>egress_optimization</td>
<td>Displays information about connections eligible for egress optimization, a feature that enhances performance. Use this command on the advice of Cisco TAC. This command uses flags F (only the forward flow is eligible for egress optimization), R (only the reverse flow is eligible), or FR (both forward and reverse flows are eligible).</td>
</tr>
<tr>
<td>finin</td>
<td>FIN inbound connections.</td>
</tr>
<tr>
<td>finout</td>
<td>FIN outbound connections.</td>
</tr>
<tr>
<td>h225</td>
<td>H.225 connections</td>
</tr>
<tr>
<td>h323</td>
<td>H.323 connections</td>
</tr>
<tr>
<td>http_get</td>
<td>HTTP get connections.</td>
</tr>
<tr>
<td>mgcp</td>
<td>MGCP connections</td>
</tr>
<tr>
<td>Keyword</td>
<td>Connection Type Displayed</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>nojava</td>
<td>Connections that deny access to Java applets.</td>
</tr>
<tr>
<td>rpc</td>
<td>RPC connections.</td>
</tr>
<tr>
<td>service_module</td>
<td>Connections being scanned by an SSM.</td>
</tr>
<tr>
<td>sip</td>
<td>SIP connections.</td>
</tr>
<tr>
<td>skinny</td>
<td>SCCP connections.</td>
</tr>
<tr>
<td>smtp_data</td>
<td>SMTP mail data connections.</td>
</tr>
<tr>
<td>sqlnet_fixup_data</td>
<td>SQL*Net data inspection engine connections.</td>
</tr>
<tr>
<td>tcp_embryonic</td>
<td>TCP embryonic connections.</td>
</tr>
<tr>
<td>vpn_orphan</td>
<td>Orphaned VPN tunneled flows.</td>
</tr>
</tbody>
</table>

When you use the `detail` option, the system displays information about the translation type and interface information using the connection flags defined in the following table.

### Table 22: Connection Flags

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>awaiting outside ACK to SYN</td>
</tr>
<tr>
<td>A</td>
<td>awaiting inside ACK to SYN</td>
</tr>
<tr>
<td>b</td>
<td>TCP state bypass</td>
</tr>
<tr>
<td>B</td>
<td>initial SYN from outside</td>
</tr>
<tr>
<td>C</td>
<td>Computer Telephony Interface Quick Buffer Encoding (CTIQBE) media connection</td>
</tr>
<tr>
<td>d</td>
<td>dump</td>
</tr>
<tr>
<td>D</td>
<td>DNS</td>
</tr>
<tr>
<td>E</td>
<td>outside back connection. This is a secondary data connection that must be initiated from the inside host. For example, using FTP, after the inside client issues the PASV command and the outside server accepts, the Firepower Threat Defense preallocates an outside back connection with this flag set. If the inside client attempts to connect back to the server, then the Firepower Threat Defense denies this connection attempt. Only the outside server can use the preallocated secondary connection.</td>
</tr>
<tr>
<td>f</td>
<td>inside FIN</td>
</tr>
<tr>
<td>F</td>
<td>outside FIN</td>
</tr>
<tr>
<td>g</td>
<td>Media Gateway Control Protocol (MGCP) connection</td>
</tr>
<tr>
<td>G</td>
<td>The G flag indicates the connection is part of a group. It is set by the GRE and FTP Strict inspections to designate the control connection and all its associated secondary connections. If the control connection terminates, then all associated secondary connections are also terminated.</td>
</tr>
<tr>
<td>Flag</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>h</td>
<td>H.225</td>
</tr>
<tr>
<td>H</td>
<td>H.323</td>
</tr>
<tr>
<td>i</td>
<td>incomplete TCP or UDP connection</td>
</tr>
<tr>
<td>I</td>
<td>inbound data</td>
</tr>
<tr>
<td>k</td>
<td>Skinny Client Control Protocol (SCCP) media connection</td>
</tr>
<tr>
<td>K</td>
<td>GTP t3-response</td>
</tr>
<tr>
<td>L</td>
<td>traffic subject to LISP flow-mobility</td>
</tr>
<tr>
<td>m</td>
<td>SIP media connection</td>
</tr>
<tr>
<td>M</td>
<td>SMTP data</td>
</tr>
<tr>
<td>n</td>
<td>GUP (gatekeeper update protocol)</td>
</tr>
</tbody>
</table>
| N    | Inspected by Snort.  
  If the system is configured to preserve connections if Snort goes down (this is enabled by default), the N flag includes a number. See the configure snort command for more information.  
  • 1—This connection will be preserved if Snort goes down.  
  • 2—Snort did go down, and this connection was preserved. The connection will no longer be inspected by Snort. |
<p>| o    | Off-loaded flow. |
| O    | outbound data |
| p    | replicated (unused) |
| P    | inside back connection. This is a secondary data connection that must be initiated from the inside host. For example, using FTP, after the inside client issues the PORT command and the outside server accepts, the Firepower Threat Defense device preallocates an inside back connection with this flag set. If the outside server attempts to connect back to the client, then the device denies this connection attempt. Only the inside client can use the preallocated secondary connection. |
| q    | SQL*Net data |
| Q    | Diameter connection |
| r    | inside acknowledged FIN |
| R    | outside acknowledged FIN for TCP connection |
| R    | UDP RPC. Because each row of show conn command output represents one connection (TCP or UDP), there will be only one R flag per row. |
| s    | awaiting outside SYN |</p>
<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>awaiting inside SYN</td>
</tr>
<tr>
<td>t</td>
<td>SIP transient connection. For UDP connections, the value t indicates that it will timeout after one minute.</td>
</tr>
<tr>
<td>T</td>
<td>SIP connection. For UDP connections, the value T indicates that the connection will timeout according to the value specified using the <code>timeout sip</code> command.</td>
</tr>
<tr>
<td>u</td>
<td>STUN connection</td>
</tr>
<tr>
<td>U</td>
<td>up</td>
</tr>
<tr>
<td>v</td>
<td>M3UA connection</td>
</tr>
<tr>
<td>V</td>
<td>VPN orphan</td>
</tr>
<tr>
<td>W</td>
<td>WAAS</td>
</tr>
<tr>
<td>X</td>
<td>Inspected by a service module</td>
</tr>
<tr>
<td>y</td>
<td>For clustering, identifies a backup owner flow</td>
</tr>
<tr>
<td>Y</td>
<td>For clustering, identifies a director flow</td>
</tr>
<tr>
<td>z</td>
<td>For clustering, identifies a forwarder flow</td>
</tr>
<tr>
<td>Z</td>
<td>Cloud Web Security</td>
</tr>
</tbody>
</table>

**Note**

For connections using a DNS server, the source port of the connection may be replaced by the IP address of DNS server in the `show conn` command output.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by `app_id`, and the idle timer for each `app_id` runs independently.

Because the `app_id` expires independently, a legitimate DNS response can only pass through the Firepower Threat Defense device within a limited period of time and there is no resource build-up. However, when you enter the `show conn` command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

**Note**

When there is no TCP traffic for the period of connection inactivity timeout (by default, 1:00:00), the connection is closed and the corresponding conn flag entries are no longer displayed.

If a LAN-to-LAN/Network-Extension Mode tunnel drops and does not come back, there might be a number of orphaned tunnel flows. These flows are not torn down as a result of the tunnel going down, but all the data attempting to flow through them is dropped. The `show conn` command output shows these orphaned flows with the `V` flag.
When you use the `count` option in Versions 6.2.0.2, and 6.2.3 or later, the system displays information about the number of connections using the statuses defined in the following table.

**Table 23: Connection Status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Connections for which preserve-connection is currently enabled.</td>
</tr>
<tr>
<td>in effect</td>
<td>Connections for which preserve-connection is currently in effect.</td>
</tr>
<tr>
<td>most enabled</td>
<td>The most number of connections ever preserved.</td>
</tr>
<tr>
<td>most in effect</td>
<td>The most number of connections simultaneously preserved.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show conn` command. This example shows a TCP session connection from inside host 10.1.1.15 to the outside Telnet server at 10.10.49.10. Because there is no B flag, the connection is initiated from the inside. The “U”, “I”, and “O” flags denote that the connection is active and has received inbound and outbound data.

```
> show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags UTIOB
TCP dmz 10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags UTIOB
TCP dmz 10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIO
TCP dmz 10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0, flags Ti
TCP dmz 10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0, flags Ti
TCP dmz 10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0, flags Ti
TCP dmz 10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0, flags Ti
TCP dmz 10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0, flags Ti
```

The following is sample output from the `show conn count` command:

```
> show conn count
30 in use, 3194964 most used
Cluster:
    fwd connections: 1 in use, 52 most used
    dir connections: 7 in use, 43826206 most used
    centralized connections: 0 in use, 15 most used
Inspect Snort:
    preserve-connection: 100 enabled, 80 in effect, 400 most enabled, 300 most in effect
```
The following is sample output from the `show conn detail` command. This example shows a UDP connection from outside host 10.10.49.10 to inside host 10.1.1.15. The D flag denotes that this is a DNS connection. The number 1028 is the DNS ID over the connection.

```
> show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
B - initial SYN from outside, b - TCP state-bypass or nailed,
C - CTIQBE media, c - cluster centralized,
D - DNS, d - dump, E - outside back connection, e - semi-distributed,
F - outside FIN, f - inside FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
i - incomplete, J - GTP, j - GTP data, k - GTP t3-response
k - Skinny media, L - LISP triggered flow owner mobility,
M - SMTP data, m - SIP media, n - GUP
O - outbound data, o - offloaded,
P - inside back connection,
Q - Diameter, q - SQL*Net data,
R - outside acknowledged FIN,
S - awaiting inside SYN, t - SIP, t - SIP transient, U - up,
V - VPN orphan, W - WAAS,
X - inspected by service module,
x - per session, Y - director stub flow, y - backup stub flow,
Z - Scansafe redirection, z - forwarding stub flow
TCP outside:10.10.49.10/23 inside:10.1.1.15/1026,
  flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
  flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
  flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
  flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
  flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.22/2000,
  flags UIB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
  flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
  flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
  flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
  flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
  flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52956 inside:192.168.1.22/2000,
  flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
  flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
  flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

The following is sample output from the `show conn` command when an orphan flow exists, as indicated by the V flag:
To limit the report to those connections that have orphan flows, add the `vpn_orphan` option to the `show conn state` command, as in the following example:

```
> show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags UOVB
```

For clustering, to troubleshoot the connection flow, first see connections on all units by entering the `cluster exec show conn` command on the master unit. Look for flows that have the following flags: director (Y), backup (y), and forwarder (z). The following example shows an SSH connection from 172.18.124.187:22 to 192.168.103.131:44727 on all three devices; FTD1 has the z flag showing it is a forwarder for the connection, FTD3 has the Y flag showing it is the director for the connection, and FTD2 has no special flags showing it is the owner. In the outbound direction, the packets for this connection enter the inside interface on FTD2 and exit the outside interface. In the inbound direction, the packets for this connection enter the outside interface on FTD1 and FTD3, are forwarded over the cluster control link to FTD2, and then exit the inside interface on FTD2.

```
> cluster exec show conn
FTD1(LOCAL):**************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside 172.18.124.187:22 inside 192.168.103.131:44727, idle 0:00:00, bytes 37240828, flags z
FTD2:***********************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside 172.18.124.187:22 inside 192.168.103.131:44727, idle 0:00:00, bytes 37240828, flags UIO
FTD3:**************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside 172.18.124.187:22 inside 192.168.103.131:44727, idle 0:00:03, bytes 0, flags Y
```

The output of `show conn detail` on FTD2 shows that the most recent forwarder was FTD1:

```
> show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN, B - initial SYN from outside, b - TCP state-bypass or nailed, C - CQBE media, c - cluster centralized, D - DNS, d - dump, E - outside back connection, e - semi-distributed, F - outside FIN, f - inside FIN, G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data, i - incomplete, J - GTP, j - GTP data, K - GTP t3-response, k - Skinny media, L - LISP triggered flow owner mobility, M - SMTP data, m - SIP media, n - GUP, O - outbound data, o - offloaded, P - inside back connection,
```
Q - Diameter, q - SQL*Net data,  
R - outside acknowledged FIN,  
R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,  
s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,  
V - VPN orphan, W - WAAS,  
w - secondary domain backup,  
X - inspected by service module,  
x - per session, Y - director stub flow, y - backup stub flow,  
Z - Scansafe redirection, z - forwarding stub flow

TCP outside: 172.18.124.187/22 inside: 192.168.103.131/44727,  
flags UIO, idle 0s, uptime 25s, timeout 1h0m, bytes 1036044,  
cluster sent/rcvd bytes 0/1032983, cluster sent/rcvd total bytes 0/1080779, owners (1,255)  
Traffic received at interface outside  
Locally received: 0 (0 byte/s)  
Traffic received at interface inside  
Locally received: 3061 (122 byte/s)  

When you use the detail keyword, you can see information about Dead Connection Detection (DCD) probing, which shows how often the connection was probed by the initiator and responder. For example, the connection details for a DCD-enabled connection would look like the following:

TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,  
flags UO, idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,  
cluster sent/rcvd bytes 0/0, owners (0,255)  
Traffic received at interface dmz  
Locally received: 0 (0 byte/s)  
Traffic received at interface inside  
Locally received: 11828 (6 byte/s)  
Initiator: 10.5.4.10, Responder: 10.5.4.11  
DCD probes sent: Initiator 5, Responder 5

### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear conn</td>
<td>Clears connections.</td>
</tr>
</tbody>
</table>
show console-output

To display the currently captured console output, use the `show console-output` command.

```
> show console-output
Message #1 : Message #2 : Setting the offload CPU count to 0
Message #3 : Compiled on Fri 20-May-16 13:36 PDT by builders
Message #4 :
Total NICs found: 14
Message #5 : i354 rev03 Gigabit Ethernet @ irq255 dev 20 index 08 MAC: e865.49b8.97f1
Message #6 : ivshmem rev03 Backplane Data Interface @ index 09 MAC: 0000.0001.0002
Message #7 : en_vtun rev00 Backplane Control Interface @ index 10 MAC: 0000.0001.0001
Message #8 : en_vtun rev00 Backplane Int-Mgmt Interface @ index 11 MAC: 0000.0001.0003
Message #9 : en_vtun rev00 Backplane Ext-Mgmt Interface @ index 12 MAC: 0000.0000.0000
Message #10 : en_vtun rev00 Backplane Tap Interface @ index 13 MAC: 0000.0100.0001
Message #11 : Running Permanent Message
Message #12 : Activation Key: Message
Message #13 : 0x00000000 Message
Message #14 : 0x00000000 Message
Message #15 : 0x00000000 Message
Message #16 : 0x00000000 Message
Message #17 : 0x00000000 Message
Message #18 : The Running Activation Key is not valid, using default settings:
Message #19 : (...output truncated...)```
show coredump

To display the setting of packet-engine coredump generation, enter the `show coredump` command.

```
show coredump
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Packet-engine coredump generation is enabled by default.

This command is only available on the Firepower 2100 series. When you run this command on an unsupported platform, the system returns the following message:

```
This command is not available on this platform.
```

### Examples

The following example shows that packet-engine coredump generation is enabled.

```
> show coredump

Process Type: Coredump State:
packet-engine enabled
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure coredump</td>
<td>Enables or disables packet-engine coredump generation.</td>
</tr>
<tr>
<td>packet-engine</td>
<td></td>
</tr>
</tbody>
</table>
show counters

To display the protocol stack counters, use the show counters command.

```
show counters [all | summary | top N] [description] [detail] [protocol protocol_name
[ :counter_name]] [threshold N]
```

**Syntax Description**

- **all**: Displays the filter details.
- **:counter_name**: Specifies a counter by name.
- **description**: Display the various counters and descriptions.
- **detail**: Displays additional counters information.
- **protocol protocol_name**: Displays the counters for the specified protocol. Enter ? for a list of options.
- **summary**: Displays a counter summary.
- **threshold N**: Displays only those counters at or above the specified threshold. The range is 1 through 4294967295.
- **top N**: Displays the counters at or above the specified threshold. The range is 1 through 4294967295.

**Command Default**

The default is `show counters summary detail threshold 1`.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display the default information.

```
> show counters
Protocol  Counter                 Value  Context
IP        IN_PKTS                  785064  Summary
IP        OUT_PKTS                 19196   Summary
IP        OUT_DROP_DWN            177099  Summary
IP        TO_ARP                   785064  Summary
TCP       OUT_PKTS                 38378   Summary
TCP       SESS_CTOOD               19189   Summary
TCP       OUT_CLSD                 19189   Summary
TCP       HASH_ADD                 19189   Summary
TCP       SND_SYN                  19189   Summary
SSLERR    BAD_SIGNATURE            3       Summary
SSLDEV    NEW_CTX                  3       Summary
VFIF      BAD_VALUE                673     Summary
VFIF      NOT_FOUND                106843325 Summary
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear counters</td>
<td>Clears the protocol stack counters.</td>
</tr>
</tbody>
</table>
show cpu

To display the CPU utilization information, use the show cpu command.

```
show cpu [detailed | external | profile [dump] | system [processor_num]]
show cpu core [all | core_id]
show cpu usage [detailed | core [all | core_id]]
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>core [all</td>
<td>core_id]</td>
</tr>
<tr>
<td>detailed</td>
<td>(Optional) Displays the CPU usage internal details.</td>
</tr>
<tr>
<td>external</td>
<td>(Optional) Displays CPU usage for external processes.</td>
</tr>
<tr>
<td>profile [dump]</td>
<td>(Optional) Displays the CPU profiling data. Include the dump keyword to see a dump of the profiling data.</td>
</tr>
<tr>
<td>system [processor_num]</td>
<td>(Optional) Displays information related to the whole system. You can optionally include a processor number to see information for a specific processor. Use the command without the keyword to see the number of available processors, which are called CPUs. Processor numbers start at 0. Thus, if the output shows there are 8 CPUs, the valid numbers for your system are 0-7.</td>
</tr>
<tr>
<td>usage</td>
<td>(Optional) Displays the CPU usage. This is the default option.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The CPU usage is computed using an approximation of the load every five seconds, and by further feeding this approximation into two, following moving averages.

You can use the show cpu profile dump command in conjunction with the cpu profile activate command to collect information for TAC use in troubleshooting CPU issues. The show cpu profile dump command output is in hexadecimal format.

For the detailed and core views, it is not unusual to see a core with zero usage when overall CPU usage is low.

For the Firepower Threat Defense Virtual (Firepower NGFW Virtual), the show cpu command also shows whether the number of CPUs allotted to the VM is within the allowed limit based on the vCPU platform license limit. The status can be Compliant, Noncompliant: Over-provisioned, or Noncompliant: Under-provisioned. This information might not be accurate.
Examples

The following example shows how to display the CPU utilization:

```
> show cpu
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

The following example shows how to display detailed CPU utilization information:

```
> show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core 5 sec 1 min 5 min
Core 0 0.0 (0.0 + 0.0) 3.3 (0.0 + 3.3) 2.4 (0.0 + 2.4)
Current control point elapsed versus the maximum control point elapsed for:
  5 seconds: 99.0%; 1 minute: 99.8%; 5 minutes: 95.9%
CPU utilization of external processes for:
  5 seconds: 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%
Total CPU utilization for:
  5 seconds: 0.2%; 1 minute: 3.3%; 5 minutes: 2.5%
```

Note

The “Current control point elapsed versus the maximum control point elapsed for” statement means that the current control point load is compared to the maximum load seen within the defined time period. This is a ratio instead of an absolute number. The figure of 99% for the 5-second interval means that the current control point load is at 99% of the maximum load that is visible over this 5-second interval. If the load continues to increase all the time, then it will always remain at 100%. However, the actual CPU may still have a lot of free capacity because the maximum absolute value has not been defined.

The following example shows how to display system-level CPU usage. Note the “(2 CPU)” indication in the first line. This is the number of processors on this device.

```
> show cpu system
Linux 3.10.62-ltsi-WR6.0.0.27_standard (ftd1.example.com) 10/20/16 _x86_64_ (2 CPU)
Time CPU %usr %nice %sys %iowait %irq %soft %steal %guest %gnice %idle
15:48:26 all 50.36 0.00 10.04 0.78 0.00 0.03 0.00 0.00 0.00 38.79
```

The following table explains the fields in the `show cpu system` output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time when these numbers were determined.</td>
</tr>
<tr>
<td>CPU</td>
<td>Processor number.</td>
</tr>
<tr>
<td>%user</td>
<td>Percentage of CPU utilization that occurred while executing at the user level (application).</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
%nice | Percentage of CPU utilization that occurred while executing at the user level with nice priority.
%sys | Percentage of CPU utilization that occurred while executing at the system level (kernel). This does not include time spent servicing interrupts or softirqs. A softirq (software interrupt) is one of up to 32 enumerated software interrupts that can run on multiple CPUs at once.
%iowait | Percentage of time that the CPUs were idle when the system had an outstanding disk I/O request.
%irq | Percentage of time spent by the CPUs to service interrupts.
%soft | Percentage of time spent by the CPUs to service softirqs.
%steal | Percentage of time spent in involuntary wait by the virtual CPUs while the hypervisor was servicing another virtual processor.
%guest | Percentage of time spent by the CPUs to run a virtual processor.
%gnice | Percentage of CPU utilization that occurred while executing at the guest level with nice priority for a virtual processor.
%idle | Percentage of time that the CPUs were idle and the system did not have an outstanding disk I/O request.

The following example activates the profiler and instructs it to store 1000 samples, the default. Next, the `show cpu profile` command shows that the profiling is in progress. After waiting some time, the next `show cpu profile` command shows that profiling has completed. Finally, we use the `show cpu profile dump` command to get the results. Copy the output and provide it to Cisco Technical Support. You might need to log your SSH session to get the full output.

```
> cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt profiling and display the incomplete results.
> show cpu profile
CPU profiling currently in progress:
  Core 0: 501 out of 1000 samples collected.
  CP: 586 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt profiling and display the incomplete results.
> show cpu profile
CPU Profiling has stopped.
  Core 0 done with 1000 samples
  CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear cpu profile</td>
<td>Clears CPU profiling data.</td>
</tr>
<tr>
<td>cpu profile activate</td>
<td>Activates CPU profiling.</td>
</tr>
<tr>
<td>show counters</td>
<td>Displays the protocol stack counters.</td>
</tr>
</tbody>
</table>

---

**Cisco Firepower Threat Defense Command Reference**

454
show crashinfo

To display the contents of the crash file stored in Flash memory, enter the show crashinfo command.

```
show crashinfo  [ console  |   module number  |   save  |   webvpn  [ detailed ] ]
```

**Syntax Description**

- **console** (Optional) Show the status of crashinfo console output.
- **module number** (Optional) Displays crash information retrieved from the specified module. Indicate the module by number, for example, 1.
- **save** (Optional) Displays whether the device is configured to save crash information to Flash memory.
- **webvpn [detailed]** (Optional) Displays Firepower Threat Defense crash recovery dumps.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the crash file is from a test crash (generated from the crashinfo test command), the first string of the crash file is “: Saved_Test_Crash” and the last string is “: End_Test_Crash”. If the crash file is from a real crash, the first string of the crash file is “: Saved_Crash” and the last string is “: End_Crash”. (This includes crashes from use of the crashinfo force page-fault or crashinfo force watchdog commands).

Compliance with FIPS 140-2 prohibits the distribution of Critical Security Parameters (keys, passwords, etc.) outside of the crypto boundary (chassis). When the device crashes, due to an assert or checkheaps failure, it is possible that the stack or memory regions dumped to the console contain sensitive data. This output must be suppressed in FIPS-mode.

**Examples**

The following example shows that there are no crashinfo information.

```
> show crashinfo
------------------ show crashinfo module 1 ------------------
INFO: This module has no crashinfo available.
```

The following example shows how to display the current crash information configuration:

```
> show crashinfo save
crashinfo save enable
```

The following example shows the status of crashinfo console output.

```
> show crashinfo console
crashinfo console enable
```
The following example shows the output for a crash file test. This test does not actually crash the Firepower Threat Defense device. It provides a simulated example file.

```bash
> crashinfo test
> show crashinfo
: Saved_Test_Crash
Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
(...Remaining output truncated...)
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crashinfo</td>
<td>Deletes the contents of the crash file.</td>
</tr>
<tr>
<td>crashinfo force</td>
<td>Forces a crash of the Firepower Threat Defense device.</td>
</tr>
<tr>
<td>crashinfo test</td>
<td>Tests the ability of the Firepower Threat Defense device to save crash information to a file in flash memory.</td>
</tr>
</tbody>
</table>
show crypto accelerator load-balance

To display the accelerator-specific load-balancing information from the hardware crypto accelerator MIB, use the `show crypto accelerator load-balance` command.

```
show crypto accelerator load-balance [ipsec | ssl | detail [ipsec | ssl]]
```

**Syntax Description**
- **detail** (Optional) Displays detailed information. You can include the `ipsec` or `ssl` keyword after this option.
- **ipsec** (Optional) Displays crypto accelerator IPSec load balancing details.
- **ssl** (Optional) Displays crypto accelerator SSL load balancing details.

**Command History**
- **Release**: 6.1
  - **Modification**: This command was introduced.

**Examples**
The following example shows global crypto accelerator load balancing statistics:

```
> show crypto accelerator load-balance

Crypto IPSEC Load Balancing Stats:
-----------------------------------

<table>
<thead>
<tr>
<th>Engine</th>
<th>Crypto Cores</th>
<th>IPSEC Sessions</th>
<th>Active Session Distribution (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>IPSEC 1, SSL 1</td>
<td>Total: 0</td>
<td>Active: 0</td>
</tr>
</tbody>
</table>

Commands Completed: 1 second 5 second 60 second
Engine 0 (load): 0.0% 0.0% 0.0%

Encrypted Data:
- Engine 0 (load): 0.0% 0.0% 0.0%

Decrypted Data:
- Engine 0 (load): 0.0% 0.0% 0.0%

Engine 0 Per Core Load Balancing Stats:
---------------------------------------

<table>
<thead>
<tr>
<th>IPSec ring 0 (load)</th>
<th>Commands Completed</th>
<th>1 second</th>
<th>5 second</th>
<th>60 second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine 0 (load)</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td></td>
</tr>
</tbody>
</table>

Encrypted Data:
- IPSec ring 0 (load): 0.0% 0.0% 0.0%
### Decrypted Data

<table>
<thead>
<tr>
<th></th>
<th>1 second</th>
<th>5 second</th>
<th>60 second</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec ring 0 (load)</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

**Crypto SSL Load Balancing Stats:**

<table>
<thead>
<tr>
<th>Engine</th>
<th>Crypto Cores</th>
<th>SSL Sessions</th>
<th>Active Session Distribution (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>IPSEC 1, SSL 1</td>
<td>Total: 0</td>
<td>Active: 0</td>
</tr>
</tbody>
</table>

#### Commands Completed

<table>
<thead>
<tr>
<th>Engine</th>
<th>1 second</th>
<th>5 second</th>
<th>60 second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine 0 (load)</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

#### Encrypted Data

<table>
<thead>
<tr>
<th>Engine</th>
<th>1 second</th>
<th>5 second</th>
<th>60 second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine 0 (load)</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

#### Decrypted Data

<table>
<thead>
<tr>
<th>Engine</th>
<th>1 second</th>
<th>5 second</th>
<th>60 second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine 0 (load)</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

**Engine 0 Per Core Load Balancing Stats:**

<table>
<thead>
<tr>
<th>Engine</th>
<th>1 second</th>
<th>5 second</th>
<th>60 second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin ring 0 (load)</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crypto accelerator statistics</td>
<td>Clears the global and accelerator-specific statistics in the crypto accelerator MIB.</td>
</tr>
<tr>
<td>clear crypto protocol statistics</td>
<td>Clears the protocol-specific statistics in the crypto accelerator MIB.</td>
</tr>
<tr>
<td>show crypto protocol statistics</td>
<td>Displays the protocol-specific statistics from the crypto accelerator MIB.</td>
</tr>
</tbody>
</table>
show crypto accelerator statistics

To display the global and accelerator-specific statistics from the hardware crypto accelerator MIB, use the `show crypto accelerator statistics` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output statistics are defined as follows:

Accelerator 0 shows statistics for the software-based crypto engine.

Accelerator 1 shows statistics for the hardware-based crypto engine.

RSA statistics show RSA operations for 2048-bit keys, which are executed in software by default. This means that when you have a 2048-bit key, IKE/SSL VPN performs RSA operations in software during the IPsec/SSL negotiation phase. Actual IPsec/SSL traffic is still processed using hardware. This may cause high CPU if there are many simultaneous sessions starting at the same time, which may result in multiple RSA key operations and high CPU. If you run into a high CPU condition because of this, then you should use a 1024-bit key to process RSA key operations in hardware. To do so, you must reenroll the identity certificate. In releases 8.3(2) or later, you can also use the crypto engine large-mod-accel command on the 5510-5550 platforms to perform these operations in hardware.

If you are using a 2048-bit RSA key and the RSA processing is performed in software, you can use CPU profiling to determine which functions are causing high CPU usage. Generally, the bn_* and BN_* functions are math operations on the large data sets used for RSA, and are the most useful when examining CPU usage during an RSA operation in software. For example:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  36.50%  :  _bn_mul_add_words
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  19.75%  :  _bn_sqr_comba8
```

Diffie-Hellman statistics show that any crypto operation with a modulus size greater than 1024 is performed in software (for example, DH5 (Diffie-Hellman group 5 uses 1536)). If so, a 2048-bit key certificate will be processed in software, which can result in high CPU usage when a lot of sessions are running.

DSA statistics show key generation in two phases. The first phase is a choice of algorithm parameters, which may be shared between different users of the system. The second phase computes private and public keys for a single user.

SSL statistics show records for the processor-intensive public key encryption algorithms involved in SSL transactions to the hardware crypto accelerator.

RNG statistics show records for a sender and receiver, which can generate the same set of random numbers automatically to use as keys.

**Examples**

The following example shows global crypto accelerator statistics:
show crypto accelerator statistics

Crypto Accelerator Status
------------------------
[Capacity]
  Supports hardware crypto: True
  Supports modular hardware crypto: False
  Max accelerators: 1
  Max crypto throughput: 100 Mbps
  Max crypto connections: 750
[Global Statistics]
  Number of active accelerators: 1
  Number of non-operational accelerators: 0
  Input packets: 700
  Input bytes: 753488
  Output packets: 700
  Output error packets: 0
  Output bytes: 767496
[Accelerator 0]
  Status: Active
  Software crypto engine
  Slot: 0
  Active time: 167 seconds
  Total crypto transforms: 7
  Total dropped packets: 0
[Input statistics]
  Input packets: 0
  Input bytes: 0
  Input hashed packets: 0
  Input hashed bytes: 0
  Decrypted packets: 0
  Decrypted bytes: 0
[Output statistics]
  Output packets: 0
  Output bad packets: 0
  Output bytes: 0
  Output hashed packets: 0
  Output hashed bytes: 0
  Encrypted packets: 0
  Encrypted bytes: 0
[Diffie-Hellman statistics]
  Keys generated: 0
  Secret keys derived: 0
[RSA statistics]
  Keys generated: 0
  Signatures: 0
  Verifications: 0
  Encrypted packets: 0
  Encrypted bytes: 0
  Decrypted packets: 0
  Decrypted bytes: 0
[DSA statistics]
  Keys generated: 0
  Signatures: 0
  Verifications: 0
[SSL statistics]
  Outbound records: 0
  Inbound records: 0
[RNG statistics]
  Random number requests: 98
  Random number request failures: 0
[Accelerator 1]
  Status: Active
Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)

Boot microcode : CNlite-MC-Boot-Cisco-1.2
SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
IPsec microcode : CNlite-MC-IPSECM-MAIN-2.03

Slot: 1
Active time: 170 seconds
Total crypto transforms: 1534
Total dropped packets: 0

[Input statistics]
  Input packets: 700
  Input bytes: 753544
  Input hashed packets: 700
  Input hashed bytes: 736400
  Decrypted packets: 700
  Decrypted bytes: 719944

[Output statistics]
  Output packets: 700
  Output bad packets: 0
  Output bytes: 767552
  Output hashed packets: 700
  Output hashed bytes: 744800
  Encrypted packets: 700
  Encrypted bytes: 728352

[Diffie-Hellman statistics]
  Keys generated: 97
  Secret keys derived: 1

[RSA statistics]
  Keys generated: 0
  Signatures: 0
  Verifications: 0
  Encrypted packets: 0
  Encrypted bytes: 0
  Decrypted packets: 0
  Decrypted bytes: 0

[DSA statistics]
  Keys generated: 0
  Signatures: 0
  Verifications: 0

[SSL statistics]
  Outbound records: 0
  Inbound records: 0

[RNG statistics]
  Random number requests: 1
  Random number request failures: 0

The following table explains the output.

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity</td>
<td>This section pertains to the crypto acceleration that the Firepower Threat Defense device can support.</td>
</tr>
<tr>
<td>Supports hardware crypto</td>
<td>(True/False) The Firepower Threat Defense device can support hardware crypto acceleration.</td>
</tr>
<tr>
<td>Supports modular hardware crypto</td>
<td>(True/False) Any supported hardware crypto accelerator can be inserted as a separate plug-in card or module.</td>
</tr>
<tr>
<td>Max accelerators</td>
<td>The maximum number of hardware crypto accelerators that the Firepower Threat Defense device supports.</td>
</tr>
</tbody>
</table>
### show crypto accelerator statistics

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac crypto throughput</td>
<td>The maximum rated VPN throughput for the device.</td>
</tr>
<tr>
<td>Max crypto connections</td>
<td>The maximum number of supported VPN tunnels for the device.</td>
</tr>
<tr>
<td>Global Statistics</td>
<td>This section pertains to the combined hardware crypto accelerators in the device.</td>
</tr>
<tr>
<td>Number of active accelerators</td>
<td>The number of active hardware accelerators. An active hardware accelerator has been initialized and is available to process crypto commands.</td>
</tr>
<tr>
<td>Number of non-operational accelerators</td>
<td>The number of inactive hardware accelerators. An inactive hardware accelerator has been detected, but either has not completed initialization or has failed and is no longer usable.</td>
</tr>
<tr>
<td>Input packets</td>
<td>The number of inbound packets processed by all hardware crypto accelerators.</td>
</tr>
<tr>
<td>Input bytes</td>
<td>The number of bytes of data in the processed inbound packets.</td>
</tr>
<tr>
<td>Output packets</td>
<td>The number of outbound packets processed by all hardware crypto accelerators.</td>
</tr>
<tr>
<td>Output error packets</td>
<td>The number of outbound packets processed by all hardware crypto accelerators in which an error has been detected.</td>
</tr>
<tr>
<td>Output bytes</td>
<td>The number of bytes of data in the processed outbound packets.</td>
</tr>
<tr>
<td>Accelerator 0</td>
<td>Each of these sections pertains to a crypto accelerator. The first one (Accelerator 0) is always the software crypto engine. Although not a hardware accelerator, the Firepower Threat Defense uses it to perform specific crypto tasks, and its statistics appear here. Accelerators 1 and higher are always hardware crypto accelerators.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the accelerator, which indicates whether the accelerator is being initialized, is active, or has failed.</td>
</tr>
<tr>
<td>Software crypto engine</td>
<td>The type of accelerator and firmware version (if applicable).</td>
</tr>
<tr>
<td>Slot</td>
<td>The slot number of the accelerator (if applicable).</td>
</tr>
<tr>
<td>Active time</td>
<td>The length of time that the accelerator has been in the active state.</td>
</tr>
<tr>
<td>Total crypto transforms</td>
<td>The total number of crypto commands that were performed by the accelerator.</td>
</tr>
<tr>
<td>Total dropped packets</td>
<td>The total number of packets that were dropped by the accelerator because of errors.</td>
</tr>
<tr>
<td>Input statistics</td>
<td>This section pertains to input traffic that was processed by the accelerator. Input traffic is considered to be ciphertext that must be decrypted and/or authenticated.</td>
</tr>
<tr>
<td>Output</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Input packets</td>
<td>The number of input packets that have been processed by the accelerator.</td>
</tr>
<tr>
<td>Input bytes</td>
<td>The number of input bytes that have been processed by the accelerator.</td>
</tr>
<tr>
<td>Input hashed packets</td>
<td>The number of packets for which the accelerator has performed hash operations.</td>
</tr>
<tr>
<td>Input hashed bytes</td>
<td>The number of bytes over which the accelerator has performed hash operations.</td>
</tr>
<tr>
<td>Decrypted packets</td>
<td>The number of packets for which the accelerator has performed symmetric decryption operations.</td>
</tr>
<tr>
<td>Decrypted bytes</td>
<td>The number of bytes over which the accelerator has performed symmetric decryption operations.</td>
</tr>
<tr>
<td>Output statistics</td>
<td>This section pertains to output traffic that has been processed by the accelerator. Input traffic is considered clear text that must be encrypted and/or hashed.</td>
</tr>
<tr>
<td>Output packets</td>
<td>The number of output packets that have been processed by the accelerator.</td>
</tr>
<tr>
<td>Output bad packets</td>
<td>The number of output packets that have been processed by the accelerator in which an error has been detected.</td>
</tr>
<tr>
<td>Output bytes</td>
<td>The number of output bytes that have been processed by the accelerator.</td>
</tr>
<tr>
<td>Output hashed packets</td>
<td>The number of packets for which the accelerator has performed outbound hash operations.</td>
</tr>
<tr>
<td>Output hashed bytes</td>
<td>The number of bytes over which the accelerator has performed outbound hash operations.</td>
</tr>
<tr>
<td>Encrypted packets</td>
<td>The number of packets for which the accelerator has performed symmetric encryption operations.</td>
</tr>
<tr>
<td>Encrypted bytes</td>
<td>The number of bytes over which the accelerator has performed symmetric encryption operations.</td>
</tr>
<tr>
<td>Diffie-Hellman statistics</td>
<td>This section pertains to Diffie-Hellman key exchange operations.</td>
</tr>
<tr>
<td>Keys generated</td>
<td>The number of Diffie-Hellman key sets that have been generated by the accelerator.</td>
</tr>
<tr>
<td>Secret keys derived</td>
<td>The number of Diffie-Hellman shared secrets that have been derived by the accelerator.</td>
</tr>
<tr>
<td>RSA statistics</td>
<td>This section pertains to RSA crypto operations.</td>
</tr>
<tr>
<td>Keys generated</td>
<td>The number of RSA key sets that have been generated by the accelerator.</td>
</tr>
<tr>
<td>Output</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Signatures</td>
<td>The number of RSA signature operations that have been performed by the accelerator.</td>
</tr>
<tr>
<td>Verifications</td>
<td>The number of RSA signature verifications that have been performed by the accelerator.</td>
</tr>
<tr>
<td>Encrypted packets</td>
<td>The number of packets for which the accelerator has performed RSA encryption operations.</td>
</tr>
<tr>
<td>Decrypted packets</td>
<td>The number of packets for which the accelerator has performed RSA decryption operations.</td>
</tr>
<tr>
<td>Decrypted bytes</td>
<td>The number of bytes of data over which the accelerator has performed RSA decryption operations.</td>
</tr>
<tr>
<td>DSA statistics</td>
<td>This section pertains to DSA operations. Note that DSA is not supported as of Version 8.2, so these statistics are no longer displayed.</td>
</tr>
<tr>
<td>Keys generated</td>
<td>The number of DSA key sets that have been generated by the accelerator.</td>
</tr>
<tr>
<td>Signatures</td>
<td>The number of DSA signature operations that have been performed by the accelerator.</td>
</tr>
<tr>
<td>Verifications</td>
<td>The number of DSA signature verifications that have been performed by the accelerator.</td>
</tr>
<tr>
<td>SSL statistics</td>
<td>This section pertains to SSL record processing operations.</td>
</tr>
<tr>
<td>Outbound records</td>
<td>The number of SSL records that have been encrypted and authenticated by the accelerator.</td>
</tr>
<tr>
<td>Inbound records</td>
<td>The number of SSL records that have been decrypted and authenticated by the accelerator.</td>
</tr>
<tr>
<td>RNG statistics</td>
<td>This section pertains to random number generation.</td>
</tr>
<tr>
<td>Random number requests</td>
<td>The number of requests to the accelerator for a random number.</td>
</tr>
<tr>
<td>Random number request failures</td>
<td>The number of random number requests to the accelerator that did not succeed.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crypto accelerator statistics</td>
<td>Clears the global and accelerator-specific statistics in the crypto accelerator MIB.</td>
</tr>
<tr>
<td>clear crypto protocol statistics</td>
<td>Clears the protocol-specific statistics in the crypto accelerator MIB.</td>
</tr>
<tr>
<td>show crypto protocol statistics</td>
<td>Displays the protocol-specific statistics from the crypto accelerator MIB.</td>
</tr>
</tbody>
</table>
**show crypto ca certificates**

To display the certificates associated with a specific trustpoint or to display all the certificates installed on the system, use the `show crypto ca certificates` command.

```
show crypto ca certificates  [trustpointname]
```

**Syntax Description**

- `trustpointname` (Optional) The name of a trustpoint. If you do not specify a name, this command displays all certificates installed on the Firepower Threat Defense device.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show crypto ca certificates` command:

```
>show crypto ca certificates tpi
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = example.com
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tpi tp2
```
show crypto ca crls

To display all cached certificate revocation lists (CRLs) or to display all CRLs cached for a specified trustpoint, use the `show crypto ca crl` command.

`show crypto ca crls [trustpool | trustpoint trustpointname]`

**Syntax Description**

- `trustpoint trustpointname` (Optional) The name of a trustpoint. If you do not specify a name, this command displays all CRLs cached on the Firepower Threat Defense device.
- `trustpool` Displays all trustpool-related CRLs.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show crypto ca crl` command:

```plaintext
> show crypto ca crl trustpoint tpi
CRL Issuer Name: cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco Systems,l=Franklin,st=MA,c=US,ea=user@example.com
   LastUpdate: 19:45:53 UTC Dec 24 2004
   NextUpdate: 08:05:53 UTC Jan 1 2005
   Retrieved from CRL Distribution Point:
   http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
   Associated Trustpoints: tpi
```
show crypto ca trustpoints

To display the CA trustpoints, use the `show crypto ca trustpoints` command.

```
show crypto ca trustpoints [trustpoint_name]
```

**Syntax Description**

- `trustpoint_name` (Optional) The name of a trustpoint to display.

**Command Default**

If you do not specify a trustpoint, all trustpoints are shown.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display the CA trustpoints.

```
> show crypto ca trustpoints
Trustpoint ftd-self:
  Configured for self-signed certificate generation.
```
show crypto ca trustpool

To display the certificates that constitute the trustpool, use the `show crypto ca trustpool` command.

```
show crypto ca trustpool [detail | policy]
```

**Syntax Description**

- `detail`  
  (Optional) Displays certificate details.

- `policy`  
  (Optional) Displays the configured trustpool policy.

**Command Default**

This command shows an abbreviated display of all the trustpool certificates. When the `detail` option is specified, more information is included.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of the `show crypto ca trustpool` command includes the fingerprint value of each certificate. These values are required for removal operation.

**Examples**

The following example shows how to display the certificates in the trustpool.

```
> show crypto ca trustpool
CA Certificate
  Status: Available
  Certificate Serial Number: 6c386c409f4ff4944154635da520ed4c
  Certificate Usage: Signature
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name: cn=bxb2008-root
dc=dbb2008
dc=mycompany
dc=com
  Subject Name:
  cn=bxb2008-root
dc=bxb2008
dc=cisco
dc=com
  Validity Date:
  start date:17:21:06 EST Jan 14 2009
dc=dbb2008
dc=mycompany
dc=com
dc=com
  Validity Date:
  end date:17:31:06 EST Jan 14 2024
CA Certificate
  Status: Available
  Certificate Serial Number: 58d1c756000000000000059
  Certificate Usage: Signature
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
  cn=bxb2008-root
dc=bxb2008
dc=mycompany
dc=com
```
Subject Name:
cn=BXB2008SUB1-CA
dc=bxb2008
dc=cisco
dc=com
OCSP AIA:
CRL Distribution Points:
Validity Date:
start date:11:54:34 EST May 18 2009
end date:12:04:34 EST May 18 2011

The following example shows how to display the trustpool policy.

> show crypto ca trustpool policy
800 trustpool certificates installed
Trustpool auto import statistics:
Last import result: SUCCESS
Next scheduled import at 22:00:00 Tues Jul 21 2015
Trustpool Policy
Trustpool revocation checking is disabled
CRL cache time: 123 seconds
CRL next update field: required and forced
Automatic import of trustpool certificates is enabled
Automatic import URL: http://www.thawte.com
Download time: 22:00:00
Policy overrides:
map: map1
match:issuer-name eq cn=Mycompany Manufacturing CA
match:issuer-name eq cn=Mycompany CA
action:skip revocation-check
map: map2
match: issuer-name eq cn=mycompany Manufacturing CA
match: issuer-name eq cn=mycompany CA2
action: allowed expired certificates

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crypto ca trustpool</td>
<td>Removes all certificates from the trustpool.</td>
</tr>
</tbody>
</table>
show crypto debug-condition

To display the currently configured filters, the unmatched states, and the error states for IPsec and ISAKMP debugging messages, use the `show crypto debug-condition` command.

**show crypto debug-condition**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the filtering conditions:

```
> show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag: OFF
IPsec debug context unmatched flag: ON
IKE peer IP address filters:
  1.1.1.0/24   2.2.2.2
IKE user name filters:
  my_user
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug crypto condition</code></td>
<td>Sets filtering conditions for IPsec and ISAKMP debugging messages.</td>
</tr>
<tr>
<td><code>debug crypto condition error</code></td>
<td>Shows debugging messages whether or not filtering conditions have been specified.</td>
</tr>
<tr>
<td><code>debug crypto condition unmatched</code></td>
<td>Shows debugging messages for IPsec and ISAKMP that do not include sufficient context information for filtering.</td>
</tr>
</tbody>
</table>
show crypto ikev1

To display the information about Internet Key Exchange version 1 (IKEv1), use the `show crypto ikev1` command.

```
show crypto ikev1 {ipsec-over-tcp | sa [detail] | stats}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipsec-over-tcp</td>
<td>Displays the IPsec over TCP data.</td>
</tr>
<tr>
<td>sa [detail]</td>
<td>Displays information about the IKEv1 runtime security association (SA) database. Include the <code>detail</code> keyword to display detailed output about the SA database.</td>
</tr>
<tr>
<td>stats</td>
<td>Displays the IKEv1 statistics.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays detailed information about the SA database. If you do not include the detail keyword, only the IKE Peer, Type, Dir, Rky, and State columns are shown.

```
> show crypto ikev1 sa detail
IKE Peer   Type  Dir  Rky  State  Encrypt Hash  Auth   Lifetime
1 209.165.200.225 User Resp No  AM_Active  3des  SHA  preshrd 86400
IKE Peer   Type  Dir  Rky  State  Encrypt Hash  Auth   Lifetime
2 209.165.200.226 User Resp No  AM_ACTIVE   3des  SHA  preshrd 86400
IKE Peer   Type  Dir  Rky  State  Encrypt Hash  Auth   Lifetime
3 209.165.200.227 User Resp No  AM_ACTIVE   3des  SHA  preshrd 86400
IKE Peer   Type  Dir  Rky  State  Encrypt Hash  Auth   Lifetime
4 209.165.200.228 User Resp No  AM_ACTIVE   3des  SHA  preshrd 86400
```

The following example displays the IPsec over TCP data:

```
> show crypto ikev1 ipsec-over-tcp
Global IKEv1 IPsec over TCP Statistics
-----------------------------------------------
Embryonic connections: 0
Active connections: 0
Previous connections: 0
Inbound packets: 0
Inbound dropped packets: 0
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 0
Received ACK heart-beat packets: 0
Bad headers: 0
Bad trailers: 0
Timer failures: 0
```
The following example displays the Global IKEv1 statistics:

```
> show crypto ikev1 stats
Global IKEv1 Statistics
  Active Tunnels: 0
  Previous Tunnels: 0
  In Octets: 0
  In Packets: 0
  In Drop Packets: 0
  In Notifyys: 0
  In P2 Exchanges: 0
  In P2 Exchange Invalids: 0
  In P2 Exchange Rejects: 0
  In P2 Sa Delete Requests: 0
  Out Octets: 0
  Out Packets: 0
  Out Drop Packets: 0
  Out Notifyys: 0
  Out P2 Exchanges: 0
  Out P2 Exchange Invalids: 0
  Out P2 Exchange Rejects: 0
  Out P2 Sa Delete Requests: 0
  Initiator Tunnels: 0
  Initiator Fails: 0
  Responder Fails: 0
  System Capacity Fails: 0
  Auth Fails: 0
  Decrypt Fails: 0
  Hash Valid Fails: 0
  No Sa Fails: 0

IKEV1 Call Admission Statistics
  Max In-Negotiation SAs: 50
  In-Negotiation SAs: 0
  In-Negotiation SAs Highwater: 0
  In-Negotiation SAs Rejected: 0
```
show crypto ikev2

To display the information about Internet Key Exchange version 2 (IKEv2), use the show crypto ikev2 command.

show crypto ikev2 {sa [detail] | stats}

Syntax Description

**sa [detail]**
Displays information about the IKEv2 runtime security association (SA) database. Include the detail keyword to display detailed output about the SA database.

**stats**
Displays the IKEv2 statistics.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example displays detailed information about the SA database:

```
> show crypto ikev2 sa detail
IKEv2 SAs:
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id       Local        Remote          Status         Role
   671069399     10.0.0.0/500  10.255.255.255/500  READY INITIATOR
     Life/Active Time: 86400/188 sec
    Session-id: 1
    Status Description: Negotiation done
    Local spi: 80173A0373C2D403      Remote spi: AE8AEFA1B97DBB22
    Local id: asa
    Remote id: asa1
    Local req mess id: 8      Remote req mess id: 7
    Local next mess id: 8      Remote next mess id: 7
    Local req queued: 8      Remote req queued: 7
    Local window: 1        Remote window: 1
    DPD configured for 10 seconds, retry 2
    NAT-T is not detected
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
                ESP spi in/out: 0x242a3da5/0xe6262034
                AH spi in/out: 0x0/0x0
                CPI in/out: 0x0/0x0
    Encr: AES-GCM, keysize: 128, esp_hmac: N/A
    ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

The following example displays the IKEv2 statistics:

```
> show crypto ikev2 stats
Global IKEv2 Statistics
  Active Tunnels: 0
  Previous Tunnels: 0
  In Octets: 0
```
In Packets: 0
In Drop Packets: 0
In Drop Fragments: 0
In Notify: 0
In P2 Exchange: 0
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In IPSEC Delete: 0
In IKE Delete: 0
Out Octets: 0
Out Packets: 0
Out Drop Packets: 0
Out Drop Fragments: 0
Out Notify: 0
Out P2 Exchange: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out IPSEC Delete: 0
Out IKE Delete: 0
SAs Locally Initiated: 0
SAs Locally Initiated Failed: 0
SAs Remotely Initiated: 0
SAs Remotely Initiated Failed: 0
System Capacity Failures: 0
Authentication Failures: 0
Decrypt Failures: 0
Hash Failures: 0
Invalid SPI: 0
In Configs: 0
Out Configs: 0
In Configs Rejects: 0
Out Configs Rejects: 0
Previous Tunnels: 0
Previous Tunnels Wraps: 0
In DPD Messages: 0
Out DPD Messages: 0
Out NAT Keepalives: 0
IKE Rekey Locally Initiated: 0
IKE Rekey Remotely Initiated: 0
CHILD Rekey Locally Initiated: 0
CHILD Rekey Remotely Initiated: 0

IKEV2 Call Admission Statistics
Max Active SAs: No Limit
Max In-Negotiation SAs: 250
Cookie Challenge Threshold: Never
Active SAs: 0
In-Negotiation SAs: 0
Incoming Requests: 0
Incoming Requests Accepted: 0
Incoming Requests Rejected: 0
Outgoing Requests: 0
Outgoing Requests Accepted: 0
Outgoing Requests Rejected: 0
Rejected Requests: 0
Rejected Over Max SA limit: 0
Rejected Low Resources: 0
Rejected Reboot In Progress: 0
Cookie Challenges: 0
Cookie Challenges Passed: 0
Cookie Challenges Failed: 0
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show crypto ikev1 sa</code></td>
<td>Displays the IKEv1 runtime SA database.</td>
</tr>
<tr>
<td><code>show running-config crypto isakmp</code></td>
<td>Displays all the active ISAKMP configuration.</td>
</tr>
</tbody>
</table>
show crypto ipsec df-bit

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

**Syntax Description**

<table>
<thead>
<tr>
<th>interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies an interface name.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show crypto ipsec fragmentation</code></td>
<td>Displays the fragmentation policy for IPsec packets.</td>
</tr>
</tbody>
</table>
show crypto ipsec fragmentation

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

`show crypto ipsec fragmentation` `interface`

**Syntax Description**

- `interface` Specifies an interface name.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show crypto ipsec df-bit</code></td>
<td>Displays the DF-bit policy for a specified interface.</td>
</tr>
</tbody>
</table>
show crypto ipsec policy

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows the OSPFv3 authentication and encryption policy.

```plaintext
> show crypto ipsec policy
Crypto IPsec client security policy data
Policy name: OSPFv3-1-256
Policy refcount: 1
Policy flags: 0x00000000
SA handles:    sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound ESP SPI: 256 (0x100)
Outbound ESP SPI: 256 (0x100)
Inbound ESP Auth Key: 1234567890123456789012345678901234567890
Outbound ESP Auth Key: 1234567890123456789012345678901234567890
Inbound ESP Cipher Key: 1234567890123456789012345678901234567890
Outbound ESP Cipher Key: 1234567890123456789012345678901234567890
Transform set:   esp-aes esp-sha-hmac
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 ospf interface</td>
<td>Displays information about OSPFv3 interfaces.</td>
</tr>
<tr>
<td>show crypto sockets</td>
<td>Displays secure socket information.</td>
</tr>
</tbody>
</table>
show crypto ipsec sa

To display a list of IPsec SAs, use the `show crypto ipsec sa` command. You can also use the alternate form of this command: `show ipsec sa`.

**Syntax Description**

```
show crypto ipsec sa [assigned-address | entry | identity | inactive | map map-name | peer
peer-addr | spi | summary | user] [detail]
```

- **assigned-address** (Optional) Displays IPsec SAs for an assigned address.
- **detail** (Optional) Displays detailed error information on what is displayed.
- **entry** (Optional) Displays IPsec SAs sorted by peer address
- **identity** (Optional) Displays inactive IPsec SAs.
- **inactive** (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.
- **spi** (Optional) Displays IPsec SAs for an SPI
- **summary** (Optional) Displays IPsec SAs summary by type
- **user** (Optional) Displays IPsec SAs for a user.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays IPsec SAs that include a tunnel identified as OSPFv3.

```
> show crypto 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
  #pks encaps: 0, #pks encrypt: 0, #pks digest: 0
  #pks decaps: 1145, #pks decrypt: 1145, #pks verify: 1145
  #pks compressed: 0, #pks decompressed: 0
  #pks not compressed: 0, #pks comp failed: 0, #pks decompl failed: 0
  #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
  #FMTUs sent: 5, #FMTUs rcvd: 2, #decapsulated frags needing reassembly: 1
  #send errors: 0, #recv errors: 0
```
local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21
path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: DC15BF68

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

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

Crypto map tag: def, local addr: 10.132.0.17
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

---

**Note**

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

The following example displays IPsec SAs for a crypto map named def.

> show crypto 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
show crypto 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

The following example shows IPsec SAs for the keyword entry.

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

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

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0
local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: DC15BF68

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

outbound esp sas:
spi: 0xDc15BF68 (3692412776)
transform: esp-3des esp-md5-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 3, crypto-map: def
sa timing: remaining key lifetime (sec): 429
IV size: 8 bytes
replay detection support: Y

peer address: 10.135.1.8
Crypto map tag: def, local addr: 172.20.0.17
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
current_peer: 10.135.1.8
dynamic allocated peer ip: 0.0.0.0

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

local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 3B6F6A35

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

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

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

> show crypto 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: 386F6A35
The following examples show IPsec SAs with the keyword `identity`.

```plaintext
> show crypto ipsec sa identity
```

```plaintext
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 comp 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 comp 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`.

```plaintext
> show crypto ipsec sa identity detail
```

```plaintext
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
```
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isakmp sa</td>
<td>Clears the IKE runtime SA database.</td>
</tr>
<tr>
<td>show running-config isakmp</td>
<td>Displays all the active ISAKMP configuration.</td>
</tr>
</tbody>
</table>
show crypto ipsec stats

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example displays IPsec statistics:

```
> show crypto ipsec stats

IPsec Global Statistics
------------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
  Bytes: 4933013
  Decompressed bytes: 4933013
  Packets: 80348
  Dropped packets: 0
  Replay failures: 0
  Authentications: 80348
  Authentication failures: 0
  Decryptions: 80348
  Decryption failures: 0
  Decapsulated fragments needing reassembly: 0
Outbound
  Bytes: 4441740
  Uncompressed bytes: 4441740
  Packets: 74029
  Dropped packets: 0
  Authentications: 74029
  Authentication failures: 0
  Encryptions: 74029
  Encryption failures: 0
  Fragmentation successes: 3
  Pre-fragmentation successes: 2
  Post-fragmentation successes: 1
  Fragmentation failures: 2
  Pre-fragmentation failures: 1
  Post-fragmentation failures: 1
  Fragments created: 10
  PMTUs sent: 1
  PMTUs recv'd: 2
  Protocol failures: 0
  Missing SA failures: 0
  System capacity failures: 0
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipsec sa</td>
<td>Clears IPsec SAs or counters based on specified parameters.</td>
</tr>
<tr>
<td>show ipsec sa</td>
<td>Displays IPsec SAs based on specified parameters.</td>
</tr>
<tr>
<td>show ipsec sa summary</td>
<td>Displays a summary of IPsec SAs.</td>
</tr>
</tbody>
</table>
show crypto isakmp

To display the ISAKMP information for both IKEv1 and IKEv2, use the **show crypto isakmp** command.

```
show crypto isakmp {sa [detail] | stats}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sa [detail]</td>
<td>Displays information about the runtime security association (SA) database. Include the <strong>detail</strong> keyword to display detailed output about the SA database.</td>
</tr>
<tr>
<td>stats</td>
<td>Displays the IKEv1 and IKEv2 statistics.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **show crypto isakmp** commands combine the output of the equivalent **show crypto ikev1** and **show crypto ikev2** commands.

Following are some tips for reading the SA information.

- Rky can be No or Yes. If yes, a rekey is occurring, and a second matching SA will be in a different state until the rekey completes.
- Role is Initiator or Responder State. This is the current state of the state machine for the SA.
- State—A tunnel that is up and passing data has a value of either MM_ACTIVE or AM_ACTIVE.

**Examples**

The following example displays detailed information about the SA database.

```
> show crypto isakmp sa detail
IKE Peer Type Dir Rky State Encrypt Hash Auth Lifetime
1 209.165.200.225 User Resp No AM_Active 3des SHA preshrd 86400
2 209.165.200.226 User Resp No AM_ACTIVE 3des SHA preshrd 86400
3 209.165.200.227 User Resp No AM_ACTIVE 3des SHA preshrd 86400
4 209.165.200.228 User Resp No AM_ACTIVE 3des SHA preshrd 86400
```

The following example displays ISAKMP statistics. IKEv1 and IKEv2 are shown separately.

```
> show crypto isakmp stats
Global IKEv1 Statistics
Active Tunnels: 136
Previous Tunnels: 0
```
### IKEV1 Call Admission Statistics

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max In-Negotiation SAs:</td>
<td>50</td>
</tr>
<tr>
<td>In-Negotiation SAs:</td>
<td>0</td>
</tr>
<tr>
<td>In-Negotiation SAs Highwater:</td>
<td>0</td>
</tr>
<tr>
<td>In-Negotiation SAs Rejected:</td>
<td>0</td>
</tr>
<tr>
<td>In Drop Packets:</td>
<td>925</td>
</tr>
</tbody>
</table>

### Global IKEv2 Statistics

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Tunnels:</td>
<td>132</td>
</tr>
<tr>
<td>Previous Tunnels:</td>
<td>132</td>
</tr>
<tr>
<td>In Octets:</td>
<td>195471</td>
</tr>
<tr>
<td>In Packets:</td>
<td>1854</td>
</tr>
<tr>
<td>In Drop Packets:</td>
<td>925</td>
</tr>
<tr>
<td>In Drop Fragments:</td>
<td>0</td>
</tr>
<tr>
<td>In Notifys:</td>
<td>0</td>
</tr>
<tr>
<td>In P2 Exchange:</td>
<td>132</td>
</tr>
<tr>
<td>In P2 Exchange Invalids:</td>
<td>0</td>
</tr>
<tr>
<td>In P2 Exchange Rejects:</td>
<td>0</td>
</tr>
<tr>
<td>In IPSEC Delete:</td>
<td>0</td>
</tr>
<tr>
<td>In IKE Delete:</td>
<td>0</td>
</tr>
<tr>
<td>Out Octets:</td>
<td>119029</td>
</tr>
<tr>
<td>Out Packets:</td>
<td>796</td>
</tr>
<tr>
<td>Out Drop Packets:</td>
<td>0</td>
</tr>
<tr>
<td>Out Drop Fragments:</td>
<td>0</td>
</tr>
<tr>
<td>Out Notifys:</td>
<td>264</td>
</tr>
<tr>
<td>Out P2 Exchange:</td>
<td>0</td>
</tr>
<tr>
<td>Out P2 Exchange Invalids:</td>
<td>0</td>
</tr>
<tr>
<td>Out P2 Exchange Rejects:</td>
<td>0</td>
</tr>
<tr>
<td>Out IPSEC Delete:</td>
<td>0</td>
</tr>
<tr>
<td>Out IKE Delete:</td>
<td>0</td>
</tr>
</tbody>
</table>

### IKEV1 Call Admission Statistics

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max In-Negotiation SAs:</td>
<td>50</td>
</tr>
<tr>
<td>In-Negotiation SAs:</td>
<td>0</td>
</tr>
<tr>
<td>In-Negotiation SAs Highwater:</td>
<td>0</td>
</tr>
<tr>
<td>In-Negotiation SAs Rejected:</td>
<td>0</td>
</tr>
<tr>
<td>In Drop Packets:</td>
<td>925</td>
</tr>
</tbody>
</table>

### Global IKEv2 Statistics

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Tunnels:</td>
<td>132</td>
</tr>
<tr>
<td>Previous Tunnels:</td>
<td>132</td>
</tr>
<tr>
<td>In Octets:</td>
<td>195471</td>
</tr>
<tr>
<td>In Packets:</td>
<td>1854</td>
</tr>
<tr>
<td>In Drop Packets:</td>
<td>925</td>
</tr>
<tr>
<td>In Drop Fragments:</td>
<td>0</td>
</tr>
<tr>
<td>In Notifys:</td>
<td>0</td>
</tr>
<tr>
<td>In P2 Exchange:</td>
<td>132</td>
</tr>
<tr>
<td>In P2 Exchange Invalids:</td>
<td>0</td>
</tr>
<tr>
<td>In P2 Exchange Rejects:</td>
<td>0</td>
</tr>
<tr>
<td>In IPSEC Delete:</td>
<td>0</td>
</tr>
<tr>
<td>In IKE Delete:</td>
<td>0</td>
</tr>
<tr>
<td>Out Octets:</td>
<td>119029</td>
</tr>
<tr>
<td>Out Packets:</td>
<td>796</td>
</tr>
<tr>
<td>Out Drop Packets:</td>
<td>0</td>
</tr>
<tr>
<td>Out Drop Fragments:</td>
<td>0</td>
</tr>
<tr>
<td>Out Notifys:</td>
<td>264</td>
</tr>
<tr>
<td>Out P2 Exchange:</td>
<td>0</td>
</tr>
<tr>
<td>Out P2 Exchange Invalids:</td>
<td>0</td>
</tr>
<tr>
<td>Out P2 Exchange Rejects:</td>
<td>0</td>
</tr>
<tr>
<td>Out IPSEC Delete:</td>
<td>0</td>
</tr>
<tr>
<td>Out IKE Delete:</td>
<td>0</td>
</tr>
</tbody>
</table>

S Commands

show crypto isakmp
In Configs: 0
Out Configs: 0
In Configs Rejects: 0
Out Configs Rejects: 0
Previous Tunnels: 0
Previous Tunnels Wraps: 0
In DPD Messages: 0
Out DPD Messages: 0
Out NAT Keepalives: 0
IKE Rekey Locally Initiated: 0
IKE Rekey Remotely Initiated: 0
CHILD Rekey Locally Initiated: 0
CHILD Rekey Remotely Initiated: 0

IKEV2 Call Admission Statistics
Max Active SAs: No Limit
Max In-Negotiation SAs: 300
Cookie Challenge Threshold: 150
Active SAs: 0
In-Negotiation SAs: 0
Incoming Requests: 0
Incoming Requests Accepted: 0
Incoming Requests Rejected: 0
Outgoing Requests: 0
Outgoing Requests Accepted: 0
Outgoing Requests Rejected: 0
Rejected Requests: 0
Rejected Over Max SA limit: 0
Rejected Low Resources: 0
Rejected Reboot In Progress: 0
Cookie Challenges: 0
Cookie Challenges Passed: 0
Cookie Challenges Failed: 0

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crypto isakmp</td>
<td>Clears the IKE runtime SA database.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays all the active ISAKMP configuration.</td>
</tr>
<tr>
<td>crypto isakmp</td>
<td></td>
</tr>
</tbody>
</table>
show crypto key mypubkey

To display the key name, usage, and elliptic curve size for ECDSA or RSA keys, use the **show crypto key mypubkey** command.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show crypto key mypubkey {ecdsa</td>
<td>rsa}</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the RSA public key:

```
> show crypto key mypubkey rsa
Key pair was generated at: 18:19:26 UTC May 26 2016
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c0bf77
d651ead6 fca31c72 12064272 36f699b9 e971e198 1503ba6b f0112b63 97252a26
38827d83 cd71863e b9962da5 bb905a47 666452a1 9eb1a36e dd8aab00 0e4493f1
4422bf09 4bcfc895 a83d38a9 7b9caba6 83c9b5b2 cff251f8 a0422a68 3690c9e5
0cbbbe83b 1a8b2460 1f83b43b a9b06912 ?cc9f7f9 f596b81e e2a7bde7 8f020301
0001
>  
```
show crypto protocol statistics

To display the protocol-specific statistics in the crypto accelerator MIB, use the show crypto protocol statistics command.

**show crypto protocol statistics**  **protocol**

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>protocol</strong></th>
<th>Specifies the name of the protocol for which to display statistics. Protocol choices are as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ikev1</td>
<td>Internet Key Exchange version 1.</td>
</tr>
<tr>
<td>ikev2</td>
<td>Internet Key Exchange version 2.</td>
</tr>
<tr>
<td>ipsec</td>
<td>IP Security Phase-2 protocols.</td>
</tr>
<tr>
<td>ssl</td>
<td>Secure Sockets Layer.</td>
</tr>
<tr>
<td>ssh</td>
<td>Secure Shell protocol</td>
</tr>
<tr>
<td>srtp</td>
<td>Secure Real-time transport protocol</td>
</tr>
<tr>
<td>other</td>
<td>Reserved for new protocols.</td>
</tr>
<tr>
<td>all</td>
<td>All protocols currently supported.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays crypto accelerator statistics for all protocols:

```plaintext
  > show crypto protocol statistics all
  (IKEv1 statistics)
    Encrypt packet requests: 46
    Encapsulate packet requests: 46
    Decrypt packet requests: 40
    Decapsulate packet requests: 40
    HMAC calculation requests: 91
    SA creation requests: 1
    SA rekey requests: 3
    SA deletion requests: 3
    Next phase key allocation requests: 2
    Random number generation requests: 0
    Failed requests: 0
  (IKEv2 statistics)
    Encrypt packet requests: 0
    Encapsulate packet requests: 0
    Decrypt packet requests: 0
    Decapsulate packet requests: 0
    HMAC calculation requests: 0
    SA creation requests: 0
    SA rekey requests: 0
    SA deletion requests: 0
```
Next phase key allocation requests: 0
Random number generation requests: 0
Failed requests: 0

[IPsec statistics]
Encrypt packet requests: 700
Encapsulate packet requests: 700
Decrypt packet requests: 700
Decapsulate packet requests: 700
HMAC calculation requests: 1400
SA creation requests: 2
SA rekey requests: 0
SA deletion requests: 0
Next phase key allocation requests: 0
Random number generation requests: 0
Failed requests: 0

[SSL statistics]
Encrypt packet requests: 0
Encapsulate packet requests: 0
Decrypt packet requests: 0
Decapsulate packet requests: 0
HMAC calculation requests: 0
SA creation requests: 0
SA rekey requests: 0
SA deletion requests: 0
Next phase key allocation requests: 0
Random number generation requests: 0
Failed requests: 0

[SSH statistics are not supported]

[SRTP statistics are not supported]

[Other statistics]
Encrypt packet requests: 0
Encapsulate packet requests: 0
Decrypt packet requests: 0
Decapsulate packet requests: 0
HMAC calculation requests: 0
SA creation requests: 0
SA rekey requests: 0
SA deletion requests: 0
Next phase key allocation requests: 0
Random number generation requests: 99
Failed requests: 0

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crypto accelerator statistics</td>
<td>Clears the global and accelerator-specific statistics in the crypto accelerator MIB.</td>
</tr>
<tr>
<td>clear crypto protocol statistics</td>
<td>Clears the protocol-specific statistics in the crypto accelerator MIB.</td>
</tr>
<tr>
<td>show crypto accelerator statistics</td>
<td>Displays the global and accelerator-specific statistics from the crypto accelerator MIB.</td>
</tr>
</tbody>
</table>
show crypto sockets

To display crypto secure socket information, use the `show crypto sockets` command.

```
show crypto sockets
```

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays crypto secure socket information:

```
> show crypto sockets
Number of Crypto Socket connections 1
Gi0/1  Peers: (local): 2001:1::1
          (remote): ::
          Local Ident (addr/plen/port/prot): (2001:1::1/64/0/89)
          Remote Ident (addr/plen/port/prot): (::/0/0/89)
          IPsec Profile: "CSSU-UTF"
          Socket State: Open
          Client: "CSSU_App(UTF)" (Client State: Active)

Crypto Sockets in Listen state:
```

The following table describes the fields in the `show crypto sockets` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Crypto Socket connections</td>
<td>Number of crypto sockets in the system.</td>
</tr>
<tr>
<td>Socket State</td>
<td>This state can be Open, which means that active IPsec security associations (SAs) exist, or it can be Closed, which means that no active IPsec SAs exist.</td>
</tr>
<tr>
<td>Client</td>
<td>Application name and its state.</td>
</tr>
<tr>
<td>Flags</td>
<td>If this field says “shared,” the socket is shared with more than one tunnel interface.</td>
</tr>
<tr>
<td>Crypto Sockets in Listen state</td>
<td>Name of the crypto IPsec profile.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show crypto ipsec policy</td>
<td>Displays the crypto secure socket API installed policy information.</td>
</tr>
</tbody>
</table>
show crypto ssl

To display information about the active SSL sessions on the Firepower Threat Defense device, use the **show crypto ssl** command

```
show crypto ssl [ cache  |  ciphers  |  errors [ trace ]  |  mib [ 64 ]  |  objects ]
```

**Syntax Description**

- **cache** (Optional) Displays SSL session cache statistics.
- **ciphers** (Optional) Displays SSL ciphers available for use.
- **errors** (Optional) Displays SSL errors.
- **trace** (Optional) Displays SSL error trace information.
- **mib** (Optional) Displays SSL MIB statistics.
- **64** (Optional) Displays SSL MIB 64-bit counter statistics.
- **objects** (Optional) Displays SSL object statistics.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command shows information about the current SSLv3 or greater sessions, including the enabled cipher order, which ciphers are disabled, SSL trustpoints being used, and whether certificate authentication is enabled.

**Examples**

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

```
> show crypto ssl
Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
Certificate authentication is not enabled
```

To display SSL session cache statistics, use the **show crypto ssl cache** command

```
> show crypto ssl cache
SSL session cache statistics:
  Maximum cache size: 100  Current cache size: 0
  Cache hits: 0  Cache misses: 0
  Cache timeouts: 0  Cache full: 0
```
To display SSL cipher lists, use the `show crypto ssl cipher` command

> `show crypto ssl cipher`

Current cipher configuration:

```
default (medium):  
  ECDHE-ECDSA-AES256-GCM-SHA384  
  ECDHE-RSA-AES256-GCM-SHA384  
  DHE-RSA-AES256-GCM-SHA384  
  AES256-GCM-SHA384  
  ECDHE-ECDSA-AES128-GCM-SHA256  
  ECDHE-RSA-AES128-GCM-SHA256  
  DHE-RSA-AES128-GCM-SHA256  
  AES128-GCM-SHA256  
  DHE-RSA-AES256-SHA  
  AES256-SHA  
  DHE-RSA-AES128-SHA  
  AES128-SHA  
  DES-CBC3-SHA
```

```
tlsv1 (medium):  
  DHE-RSA-AES256-SHA  
  AES256-SHA  
  DHE-RSA-AES128-SHA  
  AES128-SHA  
  DES-CBC3-SHA
```

```
tlsv1.1 (medium):  
  DHE-RSA-AES256-SHA  
  AES256-SHA  
  DHE-RSA-AES128-SHA  
  AES128-SHA  
  DES-CBC3-SHA
```
**S Commands**

```
show crypto ssl

DHE-RSA-AES256-SHA
AES256-SHA
DHE-RSA-AES128-SHA
AES128-SHA
DES-CBC3-SHA

tls v1.2 (medium):
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256
DHE-RSA-AES256-SHA
AES256-SHA
DHE-RSA-AES128-SHA
AES128-SHA
DES-CBC3-SHA

dtls v1 (medium):
DHE-RSA-AES256-SHA
AES256-SHA
DHE-RSA-AES128-SHA
AES128-SHA
DES-CBC3-SHA
```
show ctiqbe

To display information about CTIQBE sessions established across the Firepower Threat Defense device, use the `show ctiqbe` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show ctiqbe` command under the following conditions. There is only one active CTIQBE session setup across the device. It is established between an internal CTI device (for example, a Cisco IP SoftPhone) at local address 10.0.0.99 and an external Cisco Call Manager at 172.29.1.77, where TCP port 2748 is the Cisco CallManager. The heartbeat interval for the session is 120 seconds.

```bash
> show ctiqbe
Total: 1
LOCAL FOREIGN STATE HEARTBEAT
-----------------------------------------------
1 10.0.0.99/1117 172.29.1.77/2748 1 120
-----------------------------------------------
RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
MEDIA: Device ID 27 Call ID 0
Foreign 172.29.1.99 (1028 - 1029)
Local 172.29.1.88 (26822 - 26823)
```

The CTI device has already registered with the CallManager. The device internal address and RTP listening port is PATed to 172.29.1.99 UDP port 1028. Its RTCP listening port is PATed to UDP 1029.

The line beginning with “RTP/RTCP: PAT xlates:” appears only if an internal CTI device has registered with an external CallManager and the CTI device address and ports are PATed to that external interface. This line does not appear if the CallManager is located on an internal interface, or if the internal CTI device address and ports are NATed to the same external interface that is used by the CallManager.

The output indicates a call has been established between this CTI device and another phone at 172.29.1.88. The RTP and RTCP listening ports of the other phone are UDP 26822 and 26823. The other phone locates on the same interface as the CallManager because the Firepower Threat Defense device does not maintain a CTIQBE session record associated with the second phone and CallManager. The active call leg on the CTI device side can be identified with Device ID 27 and Call ID 0.
### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>inspect ctiqbe</code></td>
<td>Enables CTIQBE application inspection.</td>
</tr>
<tr>
<td><code>show service-policy</code></td>
<td>Shows service policy information and statistics.</td>
</tr>
<tr>
<td><code>show conn</code></td>
<td>Displays the connection state for different connection types.</td>
</tr>
</tbody>
</table>
# show ctl-provider

To display the configuration of CTL providers used in unified communications, use the `show ctl-provider` command.

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>(Optional) Shows information for this CTL provider only.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to display the configuration of the CTL providers.

```
> show ctl-provider

ctl-provider my-ctl
   client interface inside address 192.168.1.55
   client interface inside address 192.168.1.56
   client username admin password qWe.oMGKmeGte1xS encrypted
   export certificate ccm-proxy
```
show curpriv

To display the current user privileges for a Diagnostic CLI session, use the `show curpriv` command:

```
show curpriv
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `show curpriv` command displays the current privilege level. Lower privilege level numbers indicate lower privilege levels.

This information does not apply to the users defined by the `configure user` command. Instead, these are the privileges of a user within the `system support diagnostic-cli` session. You cannot change these privileges.

### Examples

The following example shows how to view the privileges for the logged-in user. These privileges apply to the Diagnostic CLI; they do not apply to the ability to use configure commands. You cannot configure permissions for the `enable_1` user. These privileges are the same for both `Basic` and `Config` permissions.

```
> show curpriv
Username : enable_1
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
```
show curpriv
show d - show h

- show database, on page 505
- show ddns update, on page 506
- show debug, on page 507
- show debug, on page 508
- show dhcpd, on page 509
- show dhcprelay, on page 511
- show diameter, on page 512
- show disk, on page 513
- show disk-manager, on page 515
- show dns, on page 516
- show dns-hosts, on page 518
- show eigrp events, on page 520
- show eigrp interfaces, on page 522
- show eigrp neighbors, on page 524
- show eigrp topology, on page 528
- show eigrp traffic, on page 531
- show environment, on page 533
- show facility-alarm, on page 537
- show failover, on page 539
- show failover exec, on page 550
- show file, on page 551
- show firewall, on page 552
- show flash, on page 553
- show flow-export counters, on page 554
- show flow-offload, on page 555
- show fqdn, on page 558
- show fragment, on page 560
- show gc, on page 561
- show h225, on page 562
- show h245, on page 563
- show h323, on page 565
- show hardware-bypass, on page 566
- show high-availability config, on page 567
• show https-access-list, on page 569
show database

To display information about the system database, use the `show database` command.

```
show database { processes | slow-query-log }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>processes</code></td>
<td>Displays information about the currently running database queries.</td>
</tr>
<tr>
<td><code>slow-query-log</code></td>
<td>Displays the database slow query log.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to display database process information.

```bash
> show database processes
Database Processes:
  Id : 3
  User : barnyard
  Host : localhost
  Database : sfsnort
  Command : Sleep
  Time : 6
  State : Null
  Info : Null
```

(...Remaining output truncated...)
show ddns update

To display information on the DDNS update methods, use the `show ddns update interface` command.

```
show ddns update { interface [interface-name] | method [method-name] }
```

**Syntax Description**

- **interface [interface-name]**: Displays the methods assigned to Firepower Threat Defense interfaces. You can optionally specify an interface name to see information on that interface only.

- **method [method-name]**: Displays information on the DDNS update methods. You can optionally enter the name of a method to see information on that method only.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the DDNS method assigned to the inside interface:

```
> show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name       Update Destination
  ddns-2                  not available
>
```

The following example displays the DDNS method named ddns-2:

```
> show ddns update method ddns-2
Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config ddns</td>
<td>Displays the type and interval of all configured DDNS methods in the running configuration.</td>
</tr>
</tbody>
</table>
show debug

To show the current debugging configuration, use the `show debug` command.

```
show debug [command  [keywords]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>command</strong></td>
</tr>
<tr>
<td>(Optional) Specifies the <code>debug</code> command whose current configuration you want to view.</td>
</tr>
<tr>
<td><strong>keywords</strong></td>
</tr>
<tr>
<td>(Optional) For each command, the keywords following the command are identical to the keywords supported by the associated <code>debug</code> command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td><strong>Modification</strong></td>
</tr>
<tr>
<td>6.1</td>
</tr>
<tr>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>For each command, the keywords following the command are identical to the keywords supported by the associated <code>debug</code> command. For information about the supported syntax, enter <code>?</code> at the keyword location.</td>
</tr>
</tbody>
</table>

For example:

- `show debug ?` lists the available commands.
- `show debug tcp ?` lists keywords available for TCP debugging.

**Examples**

The following example enables TCP debugging, then shows debugging status.

```
> debug tcp
debug tcp enabled at level 1
> show debug tcp
debug tcp enabled at level 1
d debug tcp enabled at level 1 (persistent)
```

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>debug</td>
</tr>
<tr>
<td>Enables debugging.</td>
</tr>
</tbody>
</table>
show debug

To show the current debugging configuration, use the show debug command.

show debug  [command  [keywords]]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>command</td>
<td>(Optional) Specifies the debug command whose current configuration you want to view.</td>
</tr>
<tr>
<td>keywords</td>
<td>(Optional) For each command, the keywords following the command are identical to the keywords supported by the associated debug command.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

For each command, the keywords following the command are identical to the keywords supported by the associated debug command. For information about the supported syntax, enter ? at the keyword location.

For example:

- show debug ? lists the available commands.
- show debug tcp ? lists keywords available for TCP debugging.

Examples

The following example enables TCP debugging, then shows debugging status.

```bash
> debug tcp
debug tcp enabled at level 1
> show debug tcp
debug tcp enabled at level 1
debug tcp enabled at level 1 (persistent)
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug</td>
<td>Enables debugging.</td>
</tr>
</tbody>
</table>
**show dhcpd**

To view DHCP binding, state, and statistical information, use the `show dhcpd` command.

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>binding</td>
<td>Displays binding information for a given server IP address and its associated client hardware address and lease length.</td>
</tr>
<tr>
<td>IP_address</td>
<td>Shows the binding information for the specified IP address.</td>
</tr>
<tr>
<td>state</td>
<td>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.</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays statistical information, such as the number of address pools, bindings, expired bindings, malformed messages, sent messages, and received messages.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

```
> show dhcpd binding
IP Address Client-id 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. In this example, the outside interface is a DHCP client, whereas many other interfaces are acting as DHCP server.

```
> show dhcpd state
Context Configured as DHCP Server
Interface outside, Configured for DHCP CLIENT Interface insidel_2, Configured for DHCP SERVER Interface insidel_3, Configured for DHCP SERVER Interface insidel_4, Configured for DHCP SERVER Interface insidel_5, Configured for DHCP SERVER Interface insidel_6, Configured for DHCP SERVER Interface insidel_7, Configured for DHCP SERVER Interface insidel_8, Not Configured for DHCP Interface diagnostic, Not Configured for DHCP Interface inside, Configured for DHCP SERVER
```

The following is sample output from the `show dhcpd statistics` command:
> 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
DHCDFDISCOVER 1
DHCPREQUEST 2
DHCPDECLINE 0
DHCPRELEASE 0
DHCPINFORM 0

Message Sent
BOOTREPLY 0
DHCPOFFER 1
DHCPACK 1
DHCPNAK 1

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear dhcpd</td>
<td>Clears the DHCP server bindings and statistic counters.</td>
</tr>
<tr>
<td>show running-config dhcpd</td>
<td>Displays the current DHCP server configuration.</td>
</tr>
</tbody>
</table>
show dhcprelay

To view DHCP relay agent state and statistical information, use the `show dhcprelay state` command.

```
show dhcprelay (state | statistics)
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>Displays the state of the DHCP relay agent for each interface.</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays DHCP relay statistics.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

```
> 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
```

The following shows sample output for the `show dhcprelay statistics` command:

```
> 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
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear dhcprelay statistics</td>
<td>Clears the DHCP relay agent statistic counters.</td>
</tr>
<tr>
<td>show dhcpd</td>
<td>Displays DHCP server statistics and state information.</td>
</tr>
</tbody>
</table>
show diameter

To display state information for each Diameter connection, use the `show diameter` command.

```
show diameter
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To display Diameter connection state information, you must inspect Diameter traffic. To inspect Diameter traffic, you need to configure a FlexConfig in Firepower Management Center.

**Examples**

The following shows sample output for the `show diameter` command:

```
> show diameter
Total active diameter sessions: 5
Session 3638
----------
ref_count: 1 val = .; 1096298391; 2461;
Protocol : diameter Context id : 0
From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear service-policy</td>
<td>Clears service policy statistic.</td>
</tr>
</tbody>
</table>
show disk

To display the contents of the flash memory for the Firepower Threat Defense device only, use the `show disk` command.

```
show disk
show {disk0: | disk1:} [filesys | all | controller]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`{disk0:</td>
<td>disk1:`</td>
</tr>
<tr>
<td>all</td>
<td>Shows the contents of flash memory plus the file system and controller information.</td>
</tr>
<tr>
<td>controller</td>
<td>Displays the flash controller model number.</td>
</tr>
<tr>
<td>filesys</td>
<td>Shows information about the compact flash card.</td>
</tr>
</tbody>
</table>

**Command Default**

By default, this command shows file system information.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows information about the file systems.

```
> show disk
Filesystem  Size  Used  Avail  Use%  Mounted on
tmpfs       3.9G   440K  3.9G   1%    /run
tmpfs       3.9G  168K  3.9G   1%    /var/volatile
none        3.8G   9.4M  3.8G   1%    /dev
/dev/sdb1    7.4G  104M  7.3G   2%    /mnt/disk0
/dev/mapper/root 3.7G 943M  2.6G 27%   /ngfw
/dev/mapper/var   81G   4.0G  73G   6%    /home
tmpfs        3.9G    0  3.9G   0%    /dev/cgroups
```

The following is sample output from the `show disk0:` command:

```
> show disk0:
--- -- --- --length-- -----date/time------ path
 48 107030784 Oct  5 2016  02:10:26 os.img
 50 150484 Oct  6 2016  15:36:02 install.log
 11 4096 Oct  6 2016  15:58:16 log
 13 1544 Oct 13 2016  18:59:06 log/asa-appagent.log
 16 4096 Oct  6 2016  15:59:07 crypto_archive
 51 4096 Oct  6 2016  15:59:12 coredumpinfo
 52  59 Oct  6 2016  15:59:12 coredumpinfo/coredump.cfg
 53  36 Oct  6 2016  16:04:47 enable_configure
```
The following is sample output from the **show disk0: filesys** command:

```plaintext
> show disk0: filesys

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:  245
   Number of Cylinders 1022
   Sectors per Cylinder  62
   Sector Size          512
   Total Sectors       15524180
```

The following is sample output from the **show disk0: controller** command:

```plaintext
> show disk0: controller

Flash Model: ATA Micron_M500DC_MT
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dir</strong></td>
<td>Displays the directory contents.</td>
</tr>
</tbody>
</table>
show disk-manager

To display detailed disk usage information for each part of the system, including silos, low watermarks, and high watermarks, use the `show disk-manager` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

Following is an example of showing disk manager information.

```
> show disk-manager
Silo                  Used     Minimum     Maximum
Temporary Files       0 KB     499.197 MB  1.950 GB
Action Queue Results  0 KB     499.197 MB  1.950 GB
User Identity Events  0 KB     499.197 MB  1.950 GB
UI Caches            4 KB     1.462 GB    2.925 GB
Backups              0 KB     3.900 GB    9.750 GB
Updates               0 KB     5.850 GB    14.625 GB
Other Detection Engine 0 KB    2.925 GB    5.850 GB
Performance Statistics 33 KB   998.395 MB 11.700 GB
Other Events          0 KB     1.950 GB    3.900 GB
IP Reputation & URL Filtering 0 KB     2.437 GB  4.875 GB
Archives & Cores & File Logs 0 KB     3.900 GB  19.500 GB
Unified Low Priority Events 1.329 MB  4.875 GB  24.375 GB
RNA Events            0 KB     3.900 GB    15.600 GB
File Capture          0 KB     9.750 GB    19.500 GB
Unified High Priority Events 0 KB     14.625 GB 34.125 GB
IPS Events            0 KB     11.700 GB   29.250 GB
```
show dns

To show the current resolved DNS addresses for fully qualified domain name (FQDN) network objects, or the DNS server configuration on the management interface, use the **show dns** command.

**show dns [host fqdn | system]**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host fqdn</td>
<td>Displays information about the specified fully-qualified domain name (FQDN) only.</td>
</tr>
<tr>
<td>system</td>
<td>Displays the DNS servers and search domain configured for the management interface.</td>
</tr>
</tbody>
</table>

**Command Default**

If you do not include the **system** keyword, the command shows the DNS resolutions for all FQDN network objects used in access control rules.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.3</td>
<td>Support was added for FQDN-based access control rules.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the DNS configuration for the management address.

> show dns system  
search example.com  
nameserver 72.163.47.11

The following example shows the DNS resolution for FQDN network objects that are used in access control rules. FQDN objects are resolved only if they are used in rules: simply defining an object does not initiate a DNS lookup for the name.

> show dns  
Name: www.example1.com  
Address: 10.1.3.1 TTL 00:03:01  
Address: 10.1.3.3 TTL 00:00:36  
Address: 10.4.1.2 TTL 00:01:01  
Name: www.example2.com  
Address: 10.2.4.1 TTL 00:25:13  
Address: 10.5.2.1 TTL 00:25:01  
Name: server.ddns-exampleuser.com  
Address: fe80::21e:8cff:feb5:4faa TTL 00:00:41  
Address: 10.10.10.2 TTL 00:25:01

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

> show dns host www.example1.com  
Name: www.example1.com  
Address: 10.1.3.1 TTL 00:03:01
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear dns</td>
<td>Removes FQDN network object DNS resolutions.</td>
</tr>
<tr>
<td>show network</td>
<td>Displays the configuration of the management interface.</td>
</tr>
</tbody>
</table>
show dns-hosts

To show the DNS cache, use the `show dns-hosts` command. The DNS cache includes dynamically learned entries from a DNS server and manually entered names and IP addresses.

```
show dns-hosts
```

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> 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 following table explains each field.

**Table 25: show dns-hosts Fields**

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear dns-hosts</td>
<td>Clears the DNS cache.</td>
</tr>
</tbody>
</table>
show eigrp events

To display the EIGRP event log, use the show eigrp events command.

```
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 Firepower Threat Defense device 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 500.

- **type** (Optional) Displays the events that are being logged.

**Command Default**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 cannot disable the logging of DUAL FSM events.

**Examples**

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

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

```
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:

```
show eigrp events
```

Event information for AS 100: Event log is empty.

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

```
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear eigrp events</td>
<td>Clears the EIGRP event logging buffer.</td>
</tr>
</tbody>
</table>
**show eigrp interfaces**

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

```
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 Firepower Threat Defense device 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. Specifying an interface name limits the display to the specified interface.

**Command Default**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
> show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

<table>
<thead>
<tr>
<th>Interface</th>
<th>Peers</th>
<th>Xmit Queue</th>
<th>Mean</th>
<th>Pacing Time</th>
<th>Multicast</th>
<th>Pending</th>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>0</td>
<td>0/0</td>
<td>0</td>
<td>11/434</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>outside</td>
<td>1</td>
<td>0/0</td>
<td>337</td>
<td>0/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>inside</td>
<td>1</td>
<td>0/0</td>
<td>10</td>
<td>1/63</td>
<td>103</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

The following table describes the significant fields shown in the display.
### Table 26: `show eigrp interfaces` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process</td>
<td>Autonomous system number for the EIGRP routing process.</td>
</tr>
<tr>
<td>Peers</td>
<td>Number of directly-connected peers.</td>
</tr>
<tr>
<td>Xmit Queue Un/Reliable</td>
<td>Number of packets remaining in the Unreliable and Reliable transmit queues.</td>
</tr>
<tr>
<td>Mean SRTT</td>
<td>Mean smooth round-trip time interval (in seconds).</td>
</tr>
<tr>
<td>Pacing Time Un/Reliable</td>
<td>Pacing time (in seconds) used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets).</td>
</tr>
<tr>
<td>Multicast Flow Timer</td>
<td>Maximum number of seconds in which the Firepower Threat Defense device will send multicast EIGRP packets.</td>
</tr>
<tr>
<td>Pending Routes</td>
<td>Number of routes in the packets in the transmit queue waiting to be sent.</td>
</tr>
</tbody>
</table>
show eigrp neighbors

To display the EIGRP neighbor table, use the `show eigrp neighbors` command.

```
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 Firepower Threat Defense device 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. Specifying an interface name displays all neighbor table entries that were learned through that interface.

- `static` (Optional) Displays EIGRP neighbors that are statically defined.

**Command Default**

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

**Command History**

- **Release**
  - 6.1 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:

```
> 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    Ethernet1   13        0:00:41  0   11   4     20
172.16.80.28    Ethernet0   14        0:02:01  0   10   12    24
172.16.80.31    Ethernet0   12        0:02:02  0   10   5     20
```

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

**Table 27: show eigrp neighbors Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process</td>
<td>Autonomous system number for the EIGRP routing process.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the EIGRP neighbor.</td>
</tr>
</tbody>
</table>
### Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface on which the Firepower Threat Defense device receives hello packets from the neighbor.</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Length of time (in seconds) that the Firepower Threat Defense device 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. 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. If this value reaches 0, the Firepower Threat Defense device considers the neighbor unreachable.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Elapsed time (in hours:minutes: seconds) since the Firepower Threat Defense device first heard from this neighbor.</td>
</tr>
<tr>
<td>Q Count</td>
<td>Number of EIGRP packets (update, query, and reply) that the Firepower Threat Defense device is waiting to send.</td>
</tr>
<tr>
<td>Seq Num</td>
<td>Sequence number of the last update, query, or reply packet that was received from the neighbor.</td>
</tr>
<tr>
<td>SRTT</td>
<td>Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the Firepower Threat Defense device to receive an acknowledgment of that packet.</td>
</tr>
<tr>
<td>RTO</td>
<td>Retransmission timeout (in milliseconds). This is the amount of time the Firepower Threat Defense device waits before resending a packet from the retransmission queue to a neighbor.</td>
</tr>
</tbody>
</table>

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

```plaintext
> show eigrp neighbors static
EIGRP-IPv4 neighbors for process 100
Static Address     Interface
192.168.1.5         management
```

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

*Table 28: show ip eigrp neighbors static Field Descriptions*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process</td>
<td>Autonomous system number for the EIGRP routing process.</td>
</tr>
<tr>
<td>Static Address</td>
<td>IP address of the EIGRP neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the Firepower Threat Defense device receives hello packets from the neighbor.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show eigrp neighbors detail` command:

```plaintext
> show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100

<table>
<thead>
<tr>
<th>H</th>
<th>Address</th>
<th>Interface</th>
<th>Hold</th>
<th>Uptime</th>
<th>SRTT</th>
<th>RTO</th>
<th>Q</th>
<th>Seq</th>
<th>Tye</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1.1.1.3</td>
<td>Et0/0</td>
<td>12</td>
<td>00:04:48</td>
<td>1832</td>
<td>5000</td>
<td>0</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>10.4.9.5</td>
<td>Fa0/0</td>
<td>11</td>
<td>00:04:07</td>
<td>768</td>
<td>4608</td>
<td>0</td>
<td>4</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10.4.9.10</td>
<td>Fa0/0</td>
<td>13</td>
<td>1w0d</td>
<td>1</td>
<td>3000</td>
<td>0</td>
<td>6</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.4.9.6</td>
<td>Fa0/0</td>
<td>12</td>
<td>1w0d</td>
<td>1</td>
<td>3000</td>
<td>0</td>
<td>4</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

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

**Table 29: show ip eigrp neighbors details Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process</td>
<td>Autonomous system number for the EIGRP routing process.</td>
</tr>
<tr>
<td>H</td>
<td>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.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the EIGRP neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the Firepower Threat Defense device receives hello packets from the neighbor.</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Length of time (in seconds) that the Firepower Threat Defense device 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If this value reaches 0, the Firepower Threat Defense device considers the neighbor unreachable.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Elapsed time (in hours:minutes: seconds) since the Firepower Threat Defense device first heard from this neighbor.</td>
</tr>
<tr>
<td>SRTT</td>
<td>Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the Firepower Threat Defense device to receive an acknowledgment of that packet.</td>
</tr>
<tr>
<td>RTO</td>
<td>Retransmission timeout (in milliseconds). This is the amount of time the Firepower Threat Defense device waits before resending a packet from the retransmission queue to a neighbor.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Q Count</td>
<td>Number of EIGRP packets (update, query, and reply) that the Firepower Threat Defense device is waiting to send.</td>
</tr>
<tr>
<td>Seq Num</td>
<td>Sequence number of the last update, query, or reply packet that was received from the neighbor.</td>
</tr>
<tr>
<td>Version</td>
<td>The software version that the specified peer is running.</td>
</tr>
<tr>
<td>Retrans</td>
<td>The number of times that a packet has been retransmitted.</td>
</tr>
<tr>
<td>Retries</td>
<td>The number of times an attempt was made to retransmit a packet.</td>
</tr>
<tr>
<td>Restart time</td>
<td>Elapsed time (in hours:minutes:seconds) since the specified neighbor has restarted.</td>
</tr>
</tbody>
</table>
show eigrp topology

To display the EIGRP topology table, use the **show eigrp topology** command.

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>active</strong></td>
<td>(Optional) Displays only active entries in the EIGRP topology table.</td>
</tr>
<tr>
<td><strong>all-links</strong></td>
<td>(Optional) Displays all routes in the EIGRP topology table, even those that are not feasible successors.</td>
</tr>
<tr>
<td><strong>as-number</strong></td>
<td>(Optional) Specifies the autonomous system number of the EIGRP process.</td>
</tr>
<tr>
<td><strong>ip-addr</strong></td>
<td>(Optional) Defines the IP address from the topology table to display. When specified with a mask, a detailed description of the entry is provided.</td>
</tr>
<tr>
<td><strong>mask</strong></td>
<td>(Optional) Defines the network mask to apply to the ip-addr argument.</td>
</tr>
<tr>
<td><strong>pending</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>summary</strong></td>
<td>(Optional) Displays a summary of the EIGRP topology table.</td>
</tr>
<tr>
<td><strong>zero-successors</strong></td>
<td>(Optional) Displays available routes in the EIGRP topology table.</td>
</tr>
</tbody>
</table>

**Command Default**

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 History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
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 10.2.1.0 255.255.255.0, 2 successors, FD is 0
  via 10.16.80.28 (46251776/46226176), Ethernet0
  via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.2.1.0 255.255.255.0, 1 successors, FD is 307200
  via Connected, Ethernet1
```
The following table describes the significant fields shown in the displays.

**Table 30: show eigrp topology Field Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codes</td>
<td>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.</td>
</tr>
<tr>
<td>P - Passive</td>
<td>The route is known to be good and no EIGRP computations are being performed for this destination.</td>
</tr>
<tr>
<td>A - Active</td>
<td>EIGRP computations are being performed for this destination.</td>
</tr>
<tr>
<td>U - Update</td>
<td>Indicates that an update packet was sent to this destination.</td>
</tr>
<tr>
<td>Q - Query</td>
<td>Indicates that a query packet was sent to this destination.</td>
</tr>
<tr>
<td>R - Reply</td>
<td>Indicates that a reply packet was sent to this destination.</td>
</tr>
<tr>
<td>r - Reply status</td>
<td>Flag that is set after the software has sent a query and is waiting for a reply.</td>
</tr>
<tr>
<td>address mask</td>
<td>Destination IP address and mask.</td>
</tr>
<tr>
<td>successors</td>
<td>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.</td>
</tr>
<tr>
<td>FD</td>
<td>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.</td>
</tr>
<tr>
<td>via</td>
<td>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.</td>
</tr>
<tr>
<td>(cost/adv_cost)</td>
<td>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.</td>
</tr>
<tr>
<td>interface</td>
<td>The interface from which the information was learned.</td>
</tr>
</tbody>
</table>

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

```
> 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 (Ethernet0/0), 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.

```
$ 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 (Ethernet0/0), 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear eigrp topology</code></td>
<td>Clears the dynamically discovered entries from the EIGRP topology table.</td>
</tr>
</tbody>
</table>
show eigrp traffic

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

```
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 Firepower Threat Defense device only supports one EIGRP routing process, you do not need to specify the autonomous system number.

**Command History**

- **Release** Modification
  - 6.1 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:

```
> 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
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process</td>
<td>Autonomous system number for the EIGRP routing process.</td>
</tr>
<tr>
<td>Hellos sent/received</td>
<td>Number of hello packets sent and received.</td>
</tr>
<tr>
<td>Updates sent/received</td>
<td>Number of update packets sent and received.</td>
</tr>
<tr>
<td>Queries sent/received</td>
<td>Number of query packets sent and received.</td>
</tr>
<tr>
<td>Replies sent/received</td>
<td>Number of reply packets sent and received.</td>
</tr>
<tr>
<td>Acks sent/received</td>
<td>Number of acknowledgment packets sent and received.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input queue high water mark/drops</td>
<td>Number of received packets that are approaching the maximum receive threshold and number of dropped packets.</td>
</tr>
<tr>
<td>SIA-Queries sent/received</td>
<td>Stuck-in-active queries sent and received.</td>
</tr>
<tr>
<td>SIA- Replies sent/received</td>
<td>Stuck-in-active replies sent and received.</td>
</tr>
</tbody>
</table>
show environment

To display system environment information for system components, use the `show environment` command.

**Note**

This command is not supported on Firepower 2100, 4100, and 9300 series devices. Connect to the FXOS CLI and use the `show env` command instead of this command.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show environment</code></td>
<td>Displays environment information for system components.</td>
</tr>
<tr>
<td>`[alarm-contact</td>
<td>driver</td>
</tr>
</tbody>
</table>

### `alarm-contact`

(Optional) Displays the operational status of the input alarm contacts on an ISA 3000 device.

### `driver`

(Optional) Displays the environment monitoring (IPMI) driver status. The driver status can be one of the following:

- **RUNNING**—The driver is operational.
- **STOPPED**—An error has caused the driver to stop.

### `fans`

(Optional) Displays the operational status of the cooling fans. The status is one of the following:

- **OK**—The fan is operating normally.
- **Failed**—The fan has failed and should be replaced.

### `power-supplies`

(Optional) Displays the operational status of the power supplies. The status for each power supply is one of the following:

- **OK**—The power supply is operating normally.
- **Failed**—The power supply has failed and should be replaced.
- **Not Present**—The specified power supply is not installed.

The power supply redundancy status also displays. The redundancy status is one of the following:

- **OK**—The unit is operating normally with full resources.
- **Lost**—The unit has lost redundancy but is operating normally with minimum resources. Any further failures will result in a system shutdown.
- **N/A**—The unit is not configured for power supply redundancy.

### `power_consumption`

(Optional) Displays power consumption values.

### `voltage`

(Optional) Displays the values for CPU voltage channels 1-24. Excludes the operational status.
**temperature** *(Optional)* Displays the temperature and status of the processors and chassis. The temperature is given in Celsius. You can include keywords to limit the output to a specific area: **accelerator**, **chassis**, **cpu**, **io-hub**, **motherboard**, **power-supply**.

The status is one of the following:

- **OK**—The temperature is within normal operating range, which is less than 70.
- **Critical**—The temperature is outside of normal operating range. 70-80 is considered warm; 80-90 is critical, and greater than 90 is considered unrecoverable.

---

**Command Default**

All operational information, except for the driver, is displayed if no keywords are specified.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.3</td>
<td>We added the <strong>alarm-contact</strong> keyword for the ISA 3000.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can display operating environment information for the physical components in the device. This information includes the operational status of the fans and power supplies, and temperature and status of the CPUs and chassis. For ISA 3000 devices, it includes information about the input alarm contacts.

**Examples**

The following is sample generic output from the **show environment** command:

```
> show environment
Cooling Fans:
-----------------------------------
Power Supplies:
-----------------------------------
Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan)
Power Supply Unit Redundancy: OK
-----------------------------------
Left Slot (PS0): 26 C - OK    (Power Supply Temperature)
Right Slot (PS1): 27 C - OK    (Power Supply Temperature)
Cooling Fans:
-----------------------------------
Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan)
Temperature:
-----------------------------------
Processors:
-----------------------------------
Processor 1: 44.0 C - OK    (CPU1 Core Temperature)
Processor 2: 45.0 C - OK    (CPU2 Core Temperature)
Chassis:
-----------------------------------
Ambient 1: 28.0 C - OK    (Chassis Front Temperature)
Ambient 2: 40.5 C - OK    (Chassis Back Temperature)
```
Ambient 3: 28.0 C - OK (CPU1 Front Temperature)
Ambient 4: 36.50 C - OK (CPU1 Back Temperature)
Ambient 5: 34.50 C - OK (CPU2 Front Temperature)
Ambient 6: 43.25 C - OK (CPU2 Back Temperature)

Power Supplies:
--------------------------------
Left Slot (PS0): 26 C - OK (Power Supply Temperature)
Right Slot (PS1): 27 C - OK (Power Supply Temperature)

The following is sample output from the `show environment driver` command:

```
> show environment driver
Cooling Fans:
-----------------------------------
Chassis Fans:
-----------------------------------
Cooling Fan 1: 5888 RPM - OK
Cooling Fan 2: 5632 RPM - OK
Cooling Fan 3: 5888 RPM - OK
Power Supplies:
-----------------------------------
Left Slot (PS0): N/A
Right Slot (PS1): 8448 RPM - OK
Power Supplies:
-----------------------------------
Left Slot (PS0): Not Present
Right Slot (PS1): Present
Left Slot (PS0): N/A
Right Slot (PS1): 33 C - OK
Right Slot (PS1): N/A
Right Slot (PS1): 8448 RPM - OK

Temperature:
-----------------------------------
Processors:
-----------------------------------
Processor 1: 70.0 C - OK
Chassis:
-----------------------------------
Ambient 1: 36.0 C - OK (Chassis Back Temperature)
Ambient 2: 31.0 C - OK (Chassis Front Temperature)
Ambient 3: 39.0 C - OK (Chassis Back Left Temperature)
Power Supplies:
-----------------------------------
Left Slot (PS0): N/A
Right Slot (PS1): 33 C - OK

Voltage:
-----------------------------------
Channel 1: 1.168 V - (CPU Core 0.46V-1.4V)
Channel 2: 11.954 V - (12V)
Channel 3: 4.998 V - (5V)
Channel 4: 3.296 V - (3.3V)
Channel 5: 1.496 V - (DDR3 1.5V)
Channel 6: 1.048 V - (PCH 1.5V)
```

The following is a sample output from the `show environment alarm-contact` command:

```
> show environment alarm-contact
ALARM CONTACT 1
Status: not asserted
Description: external alarm contact 1
Severity: minor
Trigger: closed
```
ALARM CONTACT 2
  Status: not asserted
  Description: external alarm contact 2
  Severity: minor
  Trigger: closed

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear facility-alarm</td>
<td>De-energizes the output relay and clears the alarm state of the LED.</td>
</tr>
<tr>
<td>clear facility-alarm</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td></td>
</tr>
<tr>
<td>show facility-alarm</td>
<td>Displays status information for triggered alarms.</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the hardware and software version.</td>
</tr>
<tr>
<td>show version</td>
<td></td>
</tr>
</tbody>
</table>
show facility-alarm

To display the triggered alarms in an ISA 3000 device, use the `show facility-alarm` command.

```
show facility-alarm { relay | status [major | minor | info] }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>relay</td>
<td>Displays the alarms that have energized the alarm output relay.</td>
</tr>
<tr>
<td>status [major</td>
<td>minor</td>
</tr>
<tr>
<td></td>
<td>• major—Displays all the major severity alarms.</td>
</tr>
<tr>
<td></td>
<td>• minor—Displays all the minor severity alarms.</td>
</tr>
<tr>
<td></td>
<td>• info—Displays all the alarms. This keyword provides the same output as</td>
</tr>
<tr>
<td></td>
<td>using no keyword.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `relay` keyword to view just the alarms that have energized the alarm output relay. The output alarm relay is energized based on whether you configure the triggered alarms to activate it. Energizing the alarm output relay activates the device that you attach to it, such as a flashing light or buzzer.

Use the `status` keyword to view all the alarms that have been triggered, regardless of whether the alarm action triggered the external alarm output relay.

The following table explains the columns in the output.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The device from which the alarm was triggered. This is usually the hostname configured on the device.</td>
</tr>
<tr>
<td>Severity</td>
<td>Major or minor.</td>
</tr>
<tr>
<td>Description</td>
<td>The type of alarm triggered. For example, temperature, external alarm contact, or redundant power supply.</td>
</tr>
<tr>
<td>Relay</td>
<td>Whether the external alarm output relay was energized or de-energized. The external output alarm is triggered based on your alarm configuration.</td>
</tr>
<tr>
<td>Time</td>
<td>The timestamp of the triggered alarm.</td>
</tr>
</tbody>
</table>

**Examples**

The following is a sample output from the `show facility-alarm relay` command:
The following is a sample output from the `show facility-alarm status` command:

### show facility-alarm status info

<table>
<thead>
<tr>
<th>Source</th>
<th>Severity</th>
<th>Description</th>
<th>Relay</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>firepower</td>
<td>minor</td>
<td>external alarm contact 1 triggered</td>
<td>Energized</td>
<td>06:56:50 UTC Mon Sep 22</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>firepower</td>
<td>minor</td>
<td>Temp below Secondary Threshold</td>
<td>De-energized</td>
<td>06:56:49 UTC Mon Sep 22</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>firepower</td>
<td>major</td>
<td>Redundant pwr missing or failed</td>
<td>De-energized</td>
<td>07:00:19 UTC Mon Sep 22</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>firepower</td>
<td>major</td>
<td>Redundant pwr missing or failed</td>
<td>De-energized</td>
<td>07:00:19 UTC Mon Sep 22</td>
</tr>
</tbody>
</table>

### show facility-alarm status major

<table>
<thead>
<tr>
<th>Source</th>
<th>Severity</th>
<th>Description</th>
<th>Relay</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>firepower</td>
<td>major</td>
<td>Redundant pwr missing or failed</td>
<td>De-energized</td>
<td>07:00:19 UTC Mon Sep 22</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>firepower</td>
<td>major</td>
<td>Redundant pwr missing or failed</td>
<td>De-energized</td>
<td>07:00:19 UTC Mon Sep 22</td>
</tr>
</tbody>
</table>

### show facility-alarm status minor

<table>
<thead>
<tr>
<th>Source</th>
<th>Severity</th>
<th>Description</th>
<th>Relay</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>firepower</td>
<td>minor</td>
<td>external alarm contact 1 triggered</td>
<td>Energized</td>
<td>06:56:50 UTC Mon Sep 22</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>firepower</td>
<td>minor</td>
<td>Temp below Secondary Threshold</td>
<td>De-energized</td>
<td>06:56:49 UTC Mon Sep 22</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear facility-alarm output</td>
<td>De-energizes the output relay and clears the alarm state of the LED.</td>
</tr>
<tr>
<td>show alarm settings</td>
<td>Displays all global alarm settings.</td>
</tr>
<tr>
<td>show environment alarm-contact</td>
<td>Displays the status of the input alarm contacts.</td>
</tr>
</tbody>
</table>
show failover

To display information about the failover status of the unit, use the `show failover` command.

```
show failover  [group  num  |  history  [details]  |  interface  |  state  |  statistics]
```

**Syntax Description**

- **group  num**: Displays the running state of the specified failover group.
- **history  [details]**: Displays failover history. The failover history displays past failover state changes and the reason for the state change. This information helps with troubleshooting.
  
  Add the `details` keyword to display failover history from the peer unit. This includes failover state changes and the reason for the state change, for the peer unit.

  History information is cleared when the device is rebooted.

- **interface**: Displays failover and stateful link information.
- **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 the last reported reason for failover. The fail reason remains in the output even when the reason for failure is cleared.

- **statistics**: Displays transmit and receive packet count of failover command interface.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.3</td>
<td>The <code>history details</code> keyword was added.</td>
</tr>
<tr>
<td>6.4</td>
<td>The following object static counts were added.</td>
</tr>
<tr>
<td></td>
<td>• Rule DB B-Sync</td>
</tr>
<tr>
<td></td>
<td>• Rule DB P-Sync</td>
</tr>
<tr>
<td></td>
<td>• Rule DB Delete</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show failover` command displays the dynamic failover information, interface status, and Stateful Failover statistics.

If both IPv4 and IPv6 addresses are configured on an interface, both addresses appear in the output. Because an interface can have more than one IPv6 address configured on it, only the link-local address is displayed. If there is no IPv4 address configured on the interface, the IPv4 address in the output appears as 0.0.0.0. If there is no IPv6 address configured on an interface, the address is simply omitted from the output.

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 stateful failover 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 Firepower Threat Defense device up time, which the active Firepower Threat Defense device passes on to the standby Firepower Threat Defense device.
  • 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.
  • IPv6 ND tbl—The IPv6 neighbor discovery table 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.
  • SIP Session—SIP signalling session information.
  • Route Session—LU statistics of the route synhronization updates
  • Rule DB B-Sync—Indicates the number of times the rule database bulk sync is performed and the corresponding errors (if any)
  • Rule DB P-Sync—Indicates the number of times the rule database is periodically synced and the errors for this operation (if any)
  • Rule DB Delete—Indicates the number of times the rule database delete message is sent and the error of this operation (if any)

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.

The following table describes the interface states for failover.
Table 32: Failover Interface States

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>The interface is up and receiving hello packets from the corresponding</td>
</tr>
<tr>
<td></td>
<td>interface on the peer unit.</td>
</tr>
<tr>
<td>Normal (Waiting)</td>
<td>The interface is up but has not yet received a hello packet from the</td>
</tr>
<tr>
<td></td>
<td>corresponding interface on the peer unit. Verify that a standby IP address</td>
</tr>
<tr>
<td></td>
<td>has been configured for the interface and that there is connectivity</td>
</tr>
<tr>
<td></td>
<td>between the two interfaces.</td>
</tr>
<tr>
<td>Normal (Not-Monitored)</td>
<td>The interface is up but is not monitored by the failover process. The failure</td>
</tr>
<tr>
<td></td>
<td>of an interface that is not monitored does not trigger failover.</td>
</tr>
<tr>
<td>No Link</td>
<td>The physical link is down.</td>
</tr>
<tr>
<td>No Link (Waiting)</td>
<td>The physical link is down and the interface has not yet received a hello</td>
</tr>
<tr>
<td></td>
<td>packet from the corresponding interface on the peer unit. After restoring</td>
</tr>
<tr>
<td></td>
<td>the link, verify that a standby IP address has been configured for the</td>
</tr>
<tr>
<td></td>
<td>interface and that there is connectivity between the two interfaces.</td>
</tr>
<tr>
<td>No Link (Not-Monitored)</td>
<td>The physical link is down but is not monitored by the failover process.</td>
</tr>
<tr>
<td></td>
<td>The failure of an interface that is not monitored does not trigger failover.</td>
</tr>
<tr>
<td>Link Down</td>
<td>The physical link is up, but the interface is administratively down.</td>
</tr>
<tr>
<td>Link Down (Waiting)</td>
<td>The physical link is up, but the interface is administratively down and the</td>
</tr>
<tr>
<td></td>
<td>interface has not yet received a hello packet from the corresponding</td>
</tr>
<tr>
<td></td>
<td>interface on the peer unit. After bringing the interface up, verify that</td>
</tr>
<tr>
<td></td>
<td>a standby IP address has been configured for the interface and that there</td>
</tr>
<tr>
<td></td>
<td>is connectivity between the two interfaces.</td>
</tr>
<tr>
<td>Link Down (Not-Monitored)</td>
<td>The physical link is up, but the interface is administratively down but is</td>
</tr>
<tr>
<td></td>
<td>not monitored by the failover process. The failure of an interface that is</td>
</tr>
<tr>
<td></td>
<td>not monitored does not trigger failover.</td>
</tr>
<tr>
<td>Testing</td>
<td>The interface is in testing mode due to missed hello packets from the</td>
</tr>
<tr>
<td></td>
<td>corresponding interface on the peer unit.</td>
</tr>
<tr>
<td>Failed</td>
<td>Interface testing has failed and the interface is marked as failed. If the</td>
</tr>
<tr>
<td></td>
<td>interface failure causes the failover criteria to be met, then the interface</td>
</tr>
<tr>
<td></td>
<td>failure causes a failover to the secondary unit or failover group.</td>
</tr>
</tbody>
</table>

Examples

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

```
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On
Interface Poll frequency 5 seconds, holdtime 25 seconds
```
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKXQ7JU, Mate 9A3MF0H1CP
This host: Primary - Active
  Active time: 589 (sec)
  slot 0: empty
    Interface diagnostic (0.0.0.0): Normal (Waiting)
    Interface outside (192.168.77.1): Normal (Waiting)
    Interface inside (192.168.87.1): Normal (Waiting)
  slot 1: snort rev (1.0) status (up)
  slot 2: diskstatus rev (1.0) status (up)
Other host: Secondary - Standby Ready
  Active time: 0 (sec)
  Interface diagnostic (0.0.0.0): Normal (Waiting)
  Interface outside (0.0.0.0): Normal (Waiting)
  Interface inside (0.0.0.0): Normal (Waiting)
  slot 1: snort rev (1.0) status (up)
  slot 2: diskstatus rev (1.0) status (up)
Stateful Failover Logical Update Statistics
  Link : failover GigabitEthernet0/2 (up)

  General  45   0   44   0
  sys cmd   44   0   44   0
  up time   0    0    0   0
  RFC services   0   0    0   0
  TCP conn   0    0    0   0
  UDP conn   0    0    0   0
  ARP tbl    0    0    0   0
  Xlate_TIMEOUT   0   0    0   0
  IPv6 ND tbl    0   0    0   0
  VPN IKEv1 SA   0    0    0   0
  VPN IKEv1 P2   0    0    0   0
  VPN IKEv2 SA   0    0    0   0
  VPN IKEv2 P2   0    0    0   0
  VPN CTCP upd   0    0    0   0
  VPN SDI upd    0    0    0   0
  VPN DHCP upd   0    0    0   0
  SIP Session   0    0    0   0
  SIP Tx        0    0    0   0
  SIP Pinhole   0    0    0   0
  Route Session   0    0    0   0
  Router ID    0    0    0   0
  User-Identity 1    0    0   0
  CTS SGTNAME   0    0    0   0
  CTS PAC       0    0    0   0
  TrustSec-SXP   0    0    0   0
  IPv6 Route   0    0    0   0
  STS Table     0    0    0   0
  Rule DB B-Sync   0   0   1   0
  Rule DB P-Sync   5   0   1   0
  Rule DB Delete  12   0   5   0

Logical Update Queue Information

<table>
<thead>
<tr>
<th></th>
<th>Cur</th>
<th>Max</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recv Q:</td>
<td>0</td>
<td>10</td>
<td>44</td>
</tr>
<tr>
<td>Xmit Q:</td>
<td>0</td>
<td>11</td>
<td>238</td>
</tr>
</tbody>
</table>

The following is sample output from the show failover state command for an active-standby setup:
> `show failover state`

<table>
<thead>
<tr>
<th>State</th>
<th>Last Failure Reason</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>This host - Primary Negotiation</td>
<td>Backplane Failure</td>
<td>15:44:56 UTC Jun 20 2016</td>
</tr>
<tr>
<td>Other host - Secondary Not Detected</td>
<td>Comm Failure</td>
<td>15:36:30 UTC Jun 20 2016</td>
</tr>
</tbody>
</table>

----Configuration State----
- Sync Done

----Communication State----
- Mac set

The following table describes the output of the `show failover state` command.

**Table 33: show failover state Output Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration State</td>
<td>Displays the state of configuration synchronization.</td>
</tr>
<tr>
<td></td>
<td>The following are possible configuration states for the standby unit:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Config Syncing</strong> - <strong>STANDBY</strong>—Set while the synchronized configuration</td>
</tr>
<tr>
<td></td>
<td>is being executed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Interface Config Syncing</strong> - <strong>STANDBY</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Sync Done</strong> - <strong>STANDBY</strong>—Set when the standby unit has completed a</td>
</tr>
<tr>
<td></td>
<td>configuration synchronization from the active unit.</td>
</tr>
<tr>
<td></td>
<td>The following are possible configuration states for the active unit:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Config Syncing</strong>—Set on the active unit when it is performing a</td>
</tr>
<tr>
<td></td>
<td>configuration synchronization to the standby unit.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Interface Config Syncing</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Sync Done</strong>—Set when the active unit has completed a successful</td>
</tr>
<tr>
<td></td>
<td>configuration synchronization to the standby unit.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Ready for Config Sync</strong>—Set on the active unit when the standby unit</td>
</tr>
<tr>
<td></td>
<td>signals that it is ready to receive a configuration synchronization.</td>
</tr>
<tr>
<td>Communication State</td>
<td>Displays the status of the MAC address synchronization.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Mac set</strong>—The MAC addresses have been synchronized from the peer unit to</td>
</tr>
<tr>
<td></td>
<td>this unit.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Updated Mac</strong>—Used when a MAC address is updated and needs to be</td>
</tr>
<tr>
<td></td>
<td>synchronized to the other unit. Also used during the transition period</td>
</tr>
<tr>
<td></td>
<td>where the unit is updating the local MAC addresses synchronized from the</td>
</tr>
<tr>
<td></td>
<td>peer unit.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Displays a date and timestamp for the failure.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show failover history` command on the primary unit:

```
> show failover history

<table>
<thead>
<tr>
<th>From State</th>
<th>To State</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:29:59 UTC Nov 11 2017</td>
<td>Not Detected</td>
<td>Negotiation No Error</td>
</tr>
<tr>
<td>14:30:36 UTC Nov 11 2017</td>
<td>Negotiation</td>
<td>Cold Standby Detected an Active mate</td>
</tr>
<tr>
<td>14:30:38 UTC Nov 11 2017</td>
<td>Cold Standby</td>
<td>Sync Config Detected an Active mate</td>
</tr>
<tr>
<td>14:30:47 UTC Nov 11 2017</td>
<td>Sync Config</td>
<td>Sync File System Detected an Active mate</td>
</tr>
<tr>
<td>14:30:47 UTC Nov 11 2017</td>
<td>Sync File System</td>
<td>Bulk Sync Detected an Active mate</td>
</tr>
<tr>
<td>14:31:00 UTC Nov 11 2017</td>
<td>Bulk Sync</td>
<td>Standby Ready Detected an Active mate</td>
</tr>
<tr>
<td>14:31:39 UTC Nov 11 2017</td>
<td>Standby Ready</td>
<td>Failed Interface check This host:1 single_vf: OUTSIDE Other host:0</td>
</tr>
<tr>
<td>14:31:46 UTC Nov 11 2017</td>
<td>Failed</td>
<td>Standby Ready Interface check This host:0 Other host:0</td>
</tr>
<tr>
<td>14:33:36 UTC Nov 11 2017</td>
<td>Standby Ready</td>
<td>Just Active HELLO not heard from mate</td>
</tr>
</tbody>
</table>
```

---

**Field** | **Description**
---|---
Last Failure Reason | Displays the reason for the last reported failure. This information is not cleared, even if the failure condition is cleared. This information changes only when a failover occurs.

The following are possible fail reasons:

- **Interface Failure**—The number of interfaces that failed met the failover criteria and caused failover.
- **Comm Failure**—The failover link failed or peer is down.
- **Backplane Failure**

State | Displays the Primary/Secondary and Active/Standby status for the unit.

This host/Other host | This host indicates information for the device upon which the command was executed. Other host indicates information for the other device in the failover pair.
Just Active        Active Drain        HELLO not heard from mate
14:33:36 UTC Nov 11 2017
Active Drain       Active Applying Config        HELLO not heard from mate
14:33:36 UTC Nov 11 2017
Active Applying Config       Active Config Applied        HELLO not heard from mate
14:33:36 UTC Nov 11 2017
Active Config Applied       Active        HELLO not heard from mate

The following is sample output from the `show failover history` command on the secondary unit:

```
> show failover history

<table>
<thead>
<tr>
<th>From State</th>
<th>To State</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>17:17:29 UTC Nov 10 2017</td>
<td>Not Detected</td>
<td>Negotiation</td>
</tr>
<tr>
<td>17:18:06 UTC Nov 10 2017</td>
<td>Negotiation</td>
<td>Cold Standby</td>
</tr>
<tr>
<td>17:18:08 UTC Nov 10 2017</td>
<td>Cold Standby</td>
<td>Detected an Active mate</td>
</tr>
<tr>
<td>17:18:17 UTC Nov 10 2017</td>
<td>Sync Config</td>
<td>Sync File System</td>
</tr>
<tr>
<td>17:18:17 UTC Nov 10 2017</td>
<td>Sync File System</td>
<td>Sync File System</td>
</tr>
<tr>
<td>17:18:30 UTC Nov 10 2017</td>
<td>Bulk Sync</td>
<td>Bulk Sync</td>
</tr>
<tr>
<td>17:19:09 UTC Nov 10 2017</td>
<td>Standby Ready</td>
<td>Failed</td>
</tr>
<tr>
<td>17:19:21 UTC Nov 10 2017</td>
<td>Failed</td>
<td>Standby Ready</td>
</tr>
</tbody>
</table>

```

Each entry provides the time and date the state change occurred, the beginning state, the resulting state, and the reason for the state change. The newest entries are located at the bottom of the display. Older entries appear at the top. A maximum of 60 entries can be displayed. Once the maximum number of entries has been reached, the oldest entries are removed from the top of the output as new entries are added to the bottom.

The failure reasons include details that help in troubleshooting. These include interface check, failover state check, state progression failure and service module failure.

The following is sample output from the `show failover history details` command:
The `show failover history details` command requests the peer's failover history and prints the unit failover history along with the peer's latest failover history. If the peer does not respond within one second it displays the last collected failover history information.

The following table shows the failover states. There are two types of states—stable and transient. Stable states are states that the unit can remain in until some occurrence, such as a failure, causes a state change. A transient state is a state that the unit passes through while reaching a stable state.
### Table 34: Failover States

<table>
<thead>
<tr>
<th>States</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Failover is disabled. This is a stable state.</td>
</tr>
<tr>
<td>Failed</td>
<td>The unit is in the failed state. This is a stable state.</td>
</tr>
<tr>
<td>Negotiation</td>
<td>The unit establishes the connection with peer and negotiates with peer to determine software version compatibility and Active/Standby role. Depending upon the role that is negotiated, the unit will go through the Standby Unit States or the Active Unit States or enter the failed state. This is a transient state.</td>
</tr>
<tr>
<td>Not Detected</td>
<td>The ASA cannot detect the presence of a peer. This can happen when the ASA boots up with failover enabled but the peer is not present or is powered down.</td>
</tr>
</tbody>
</table>

#### Standby Unit States

<table>
<thead>
<tr>
<th>States</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cold Standby</td>
<td>The unit waits for the peer to reach the Active state. When the peer unit reaches the Active state, this unit progresses to the Standby Config state. This is a transient state.</td>
</tr>
<tr>
<td>Sync Config</td>
<td>The unit requests the running configuration from the peer unit. If an error occurs during the configuration synchronization, the unit returns to the Initialization state. This is a transient state.</td>
</tr>
<tr>
<td>Sync File System</td>
<td>The unit synchronizes the file system with the peer unit. This is a transient state.</td>
</tr>
<tr>
<td>Bulk Sync</td>
<td>The unit receives state information from the peer. This state only occurs when Stateful Failover is enabled. This is a transient state.</td>
</tr>
<tr>
<td>Standby Ready</td>
<td>The unit is ready to take over if the active unit fails. This is a stable state.</td>
</tr>
</tbody>
</table>

#### Active Unit States

<table>
<thead>
<tr>
<th>States</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Just Active</td>
<td>The first state the unit enters when becoming the active unit. During this state a message is sent to the peer alerting the peer that the unit is becoming active and the IP and MAC addresses are set for the interfaces. This is a transient state.</td>
</tr>
<tr>
<td>Active Drain</td>
<td>Queues messages from the peer are discarded. This is a transient state.</td>
</tr>
<tr>
<td>Active Applying Config</td>
<td>The unit is applying the system configuration. This is a transient state.</td>
</tr>
<tr>
<td>Active Config Applied</td>
<td>The unit has finished applying the system configuration. This is a transient state.</td>
</tr>
<tr>
<td>Active</td>
<td>The unit is active and processing traffic. This is a stable state.</td>
</tr>
</tbody>
</table>

Each state change is followed by a reason for the state change. The reason typically remains the same as the unit progresses through the transient states to the stable state. The following are the possible state change reasons:

- No Error
• Set by the CI config cmd
• Failover state check
• Failover interface become OK
• HELLO not heard from mate
• Other unit has different software version
• Other unit operating mode is different
• Other unit license is different
• Other unit chassis configuration is different
• Other unit card configuration is different
• Other unit want me Active
• Other unit want me Standby
• Other unit reports that I am failed
• Other unit reports that it is failed
• Configuration mismatch
• Detected an Active mate
• No Active unit found
• Configuration synchronization done
• Recovered from communication failure
• Other unit has different set of vlans configured
• Unable to verify vlan configuration
• Incomplete configuration synchronization
• Configuration synchronization failed
• Interface check
• My communication failed
• ACK not received for failover message
• Other unit got stuck in learn state after sync
• No power detected from peer
• No failover cable
• HA state progression failed
• Detect service card failure
• Service card in other unit has failed
• My service card is as good as peer
• LAN Interface become un-configured
• Peer unit just reloaded
• Switch from Serial Cable to LAN-Based fover
• Unable to verify state of config sync
• Auto-update request
• Unknown reason

The following is sample output from the `show failover interface` command. The device has an IPv6 address configured on the failover interface.

```
> show failover interface
   interface folink GigabitEthernet0/2
       System IP Address: 2001:a0a:b00::a0a:b70/64
       My IP Address    : 2001:a0a:b00::a0a:b70
       Other IP Address : 2001:a0a:b00::a0a:b71
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config failover</td>
<td>Displays the <code>failover</code> commands in the current configuration.</td>
</tr>
</tbody>
</table>
show failover exec

To display the failover exec command mode for the specified unit, use the **show failover exec** command.

```
show failover exec { active | standby | mate }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Displays the <strong>failover exec</strong> command mode for the active unit.</td>
</tr>
<tr>
<td>mate</td>
<td>Displays the <strong>failover exec</strong> command mode for the peer unit.</td>
</tr>
<tr>
<td>standby</td>
<td>Displays the <strong>failover exec</strong> command mode for the standby unit.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **failover exec** command creates a session with the specified device. By default, that session is in global configuration mode, even though Firepower Threat Defense does not support CLI configuration. The mode information is not relevant for Firepower Threat Defense.

The **show failover exec** command displays the command mode on the specified device in which commands sent with the **failover exec** command are executed.

### Examples

The following is sample output from the **show failover exec** command.

```
> show failover exec mate
Standby unit Failover EXEC is at config mode
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>failover exec</td>
<td>Executes the supplied command on the designated unit in a failover pair.</td>
</tr>
</tbody>
</table>
show file

To display information about the file system, use the `show file` command.

```
show file descriptors | system | information filename
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>descriptors</td>
<td>Displays all open file descriptors.</td>
</tr>
<tr>
<td>information</td>
<td>Displays information about the specified file, including partner application package files.</td>
</tr>
<tr>
<td>filename</td>
<td>Displays the size, bytes available, type of media, flags, and prefix information about the disk file system.</td>
</tr>
<tr>
<td>system</td>
<td>Displays the size, bytes available, type of media, flags, and prefix information about the disk file system.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show file system` command:

```
> show file system
File Systems:
<table>
<thead>
<tr>
<th>Size(b)</th>
<th>Free(b)</th>
<th>Type</th>
<th>Flags</th>
<th>Prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>7935832064</td>
<td>7828107264</td>
<td>disk</td>
<td>rw</td>
<td>disk0: flash:</td>
</tr>
</tbody>
</table>
- disk          | rw          | disk1:|
- network rw    | tftp:       |
- opaque rw     | system:     |
- network ro    | http:       |
- network ro    | https:      |
- network rw    | scp:        |
- network rw    | ftp:        |
- network wo    | cluster:    |
- stub ro       | cluster_trace:|
- network rw    | smb:        |
```

The following is sample output from the `show file information` command:

```
> show file information install.log
disk0:/install.log:
type is ascii text
file size is 150484 bytes
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dir</td>
<td>Displays the directory contents.</td>
</tr>
<tr>
<td>pwd</td>
<td>Displays the current working directory.</td>
</tr>
</tbody>
</table>
show firewall

To show the current firewall mode (routed or transparent), use the `show firewall` command.

```
show firewall
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show firewall` command:

```
> show firewall
Firewall mode: Router
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure firewall</td>
<td>Sets the firewall mode.</td>
</tr>
<tr>
<td>show mode</td>
<td>Shows the current context mode, either single or multiple.</td>
</tr>
</tbody>
</table>
show flash

To display the contents of the internal Flash memory, use the **show flash**: command.

```
show flash: [all | controller | filesys]
```

**Note**  
In Firepower Threat Defense, the **flash** keyword is aliased to **disk0**.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all Flash information.</td>
</tr>
<tr>
<td>controller</td>
<td>Displays file system controller information.</td>
</tr>
<tr>
<td>filesys</td>
<td>Displays file system information.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show flash:
---#--- --length-- -----date/time------ path
  48  107030784 Oct 05 2016 02:10:26 os.img
  49    33 Oct 06 2016 16:15:24 .boot_string
  50  150484 Oct 06 2016 15:36:02 install.log
  11  4096 Oct 06 2016 15:58:16 log
  13  1065 Oct 06 2016 15:59:13 log/asa-appagent.log
  16  4096 Oct 06 2016 15:59:07 crypto_archive
  51  4096 Oct 06 2016 15:59:12 coredumpinfo
  52    59 Oct 06 2016 15:59:12 coredumpinfo/coredump.cfg
  53    36 Oct 06 2016 16:04:47 enable_configure
7935832064 bytes total (7828107264 bytes free)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dir</td>
<td>Displays the directory contents.</td>
</tr>
<tr>
<td>show disk0:</td>
<td>Displays the contents of the internal Flash memory.</td>
</tr>
<tr>
<td>show disk1:</td>
<td>Displays the contents of the external Flash memory card.</td>
</tr>
</tbody>
</table>
show flow-export counters

To view the runtime counters for NetFlow statistical and error data, use the `show flow-export counters` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display Netflow runtime counters.

```
> show flow-export counters

destination: inside 209.165.200.224 2055
Statistics:
   packets sent 1000
Errors:
   block allocation failure 0
   invalid interface 0
   template send failure 0
   no route to collector 0
   source port allocation 0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear flow-export counters</td>
<td>Resets all runtime counters in NetFlow to zero.</td>
</tr>
</tbody>
</table>
show flow-offload

To view flows, counters, statistics, and information about offloaded flows, use the `show flow-offload` command. This command is available on Firepower Threat Defense on the Firepower 4100/9300 chassis.

```
```

### Syntax Description

**flow [ dynamic [ static ] ] [ count | detail ]**  
With no parameters, shows static and dynamic flows in use, maximum used, percent offloaded, and number of collisions.

Add the `dynamic` or `static` keyword to display counters, statistics, and information for dynamic or static flows only, respectively.

You can optionally add the following keywords:

- **count**: Number of offloaded active flows and offloaded flows created.
- **detail**: Active offloaded flows and their rewrite rules and data.

**info [ detail ]**  
Current state of dynamic flow offload. Add the `detail` keyword to get additional information such as a summary of port usage.

**statistics**  
Packet counts, successful transmissions, and errors.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `show flow-offload` command to display flows, counters, statistics, and information about flow offload.

Clear counters or statistics using the `clear flow-offload` command.

Following is example output from the `show flow-offload flow` command. A collision occurs when more than one flow access the hardware at the same time; in that case, only the first flow is offloaded.

```
>show flow-offload flow
Total offloaded flow stats: 1 in use, 5 most used, 100% offloaded, 0 collisions
UDP intfc 103 src 10.1.1.2:41110 dest 20.1.1.2:5001, dynamic, timestamp 162810457, packets 84040, bytes 127404640
```

Following is example output from the `show flow-offload flow count` command.

```
>show flow-offload flow count
Total offloaded flow stats: 4 in use, 20 most used, 10% offloaded, 0 collisions
```

Following is example output from the `show flow-offload flow detail` command. `rw(number)` indicate the standard header fields like MAC or VLAN have been rewritten for that particular offloaded flow.

```
>show flow-offload flow detail
Total offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
TCP vlan 711 intfc 101 src 172.16.1.3:21766 dest 9.9.1.3:80, dynamic, timestamp 217959066, packets 633139, bytes 43053452
  node 0, ft index 58197, queue_id 727
```
Following is example output from the `show flow-offload dynamic` command.

```plaintext
> show flow-offload dynamic
Dynamically offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
  TCP vlan 711 intfc 101 src 172.16.1.3:21809 dest 9.9.1.3:80, dynamic, timestamp 218392513,
  packets 14741, bytes 1002388
  TCP vlan 911 intfc 102 src 9.9.1.3:80 dest 172.16.1.3:21809, dynamic, timestamp 218392534,
  packets 16794, bytes 23972345
```

Following is example output from the `show flow-offload dynamic count` command.

```plaintext
> show flow-offload flow dynamic count
Dynamically offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
```

Following is example output from the `show flow-offload dynamic detail` command.

```plaintext
> show flow-offload flow dynamic detail
Total offloaded flow stats: 4 in use, 20 most used, 10% offloaded, 0 collisions
  TCP intfc 134 src 9.9.1.3:80 dest 192.168.0.3:5240, static, timestamp 142633202, packets
  442870, bytes 630432720
  TCP intfc 133 src 192.168.0.3:5240 dest 9.9.1.3:80, static, timestamp 142633204, packets
  442971, bytes 28350144
  TCP intfc 136 src 9.9.1.4:80 dest 192.168.0.4:7240, dynamic, timestamp 142633876, packets
  82870, bytes 10342730
  TCP intfc 135 src 192.168.0.4:7240 dest 9.9.1.4:80, dynamic, timestamp 142633877, packets
  82971, bytes 350144
```

Following is example output from the `show flow-offload info` command. **Current running state** is the current state of flow offload and is reserved for future implementation (the value is not currently configurable). **User configured state** is the state of flow offload if the managed device is rebooted. (Currently, these values will always be the same.) **Dynamic flow offload** is the current state of dynamic flow offload.

```plaintext
> show flow-offload info
Current running state : Enabled
User configured state : Enabled
Dynamic flow offload : Enabled
```

Following is example output from the `show flow-offload info detail` command.

```plaintext
> show flow-offload info detail
Current running state : Enabled
User configured state : Enabled
Dynamic flow offload : Enabled
Offload App : Running
Offload allocated cores : S0[ 1] S1[ 13]
Offload reserved Nic : 9 22
Max PKT burst : 32
Port-0 details :
  RX queue number : 149
  FQ queue number : 727
  Keep alive counter : 142327
Port-1 details :
  RX queue number : 147
  FQ queue number : 725
  Keep alive counter : 142328
```

Following is example output from the `show flow-offload statistics` command. **VNIC** refers to the hardware on which dynamic flows are offloaded.

```plaintext
> show flow-offload statistics
Packet stats of port : 0
  Tx Packet count : 16483549549
```
Rx Packet count : 16483549549
Dropped Packet count : 0
VNIC transmitted packet : 16483549549
VNIC transmitted bytes : 12389816183297
VNIC Dropped packets : 0
VNIC erroneous received : 0
VNIC CRC errors : 0
VNIC transmit failed : 0
VNIC multicast received : 0

**Related Commands**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure flow-offload</td>
<td>Enable or disable dynamic flow offload.</td>
</tr>
<tr>
<td>clear flow-offload</td>
<td>Clears dynamic flow offload counters or statistics.</td>
</tr>
</tbody>
</table>
show fqdn

To display troubleshooting information about fully-qualified domain name (FQDN) network object name resolution, use the show fqdn command.

```
show fqdn [id [fqdn_id] | ip [ip_address]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id [fqdn_id]</td>
<td>Displays information based on the ID number associated with the FQDN network object. The ID is assigned by the system. You can optionally include the ID value, which you can find by examining the output of the show running-config command. For example, the following object has 1001 as the ID number.</td>
</tr>
<tr>
<td>ip [ip_address]</td>
<td>Displays information based on the IP address obtained from the DNS server. You can optionally enter an IP address.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command for troubleshooting purposes. If you want to see how an FQDN maps to IP addresses, use the show dns command instead of this one.

The show fqdn command provides detailed information that ties the name resolution to the specific network object through the system-provided ID number for each object.

**Example**

The following example shows how to view FQDN mappings for object IDs and IP addresses.

```
> show fqdn

FQDN IP Table:
ip=10.1.45.1, object=Testobj-1, domain=www.cisco.com, hits=10,
     id=45893456,63987645

ip=2001::134, object=Testobj-1, domain=www.cisco.com, hits=10,
     id=45893456

FQDN ID Table:
id=45893456, object=Testobj-1, domain=www.cisco.com
     ip=10.1.45.1, ip=34.12.45.189
     ip6=2001::134

id=23987645, object=Testobj-2, domain=www.google.com
     ip=20.11.65.121, ip=101.2.4.69
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear dns</td>
<td>Removes FQDN network object DNS resolutions.</td>
</tr>
<tr>
<td>show dns</td>
<td>Displays FQDN network object DNS resolutions.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the running configuration.</td>
</tr>
</tbody>
</table>
show fragment

To display the operational data of the IP fragment reassembly module, enter the `show fragment`.

```
show fragment  [interface]
```

### Syntax Description

- `interface`  
  (Optional) Specifies the Firepower Threat Defense interface.

### Command Default

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

```
> show fragment
Interface: inside
  Size: 200, Chain: 24, Timeout: 5, Threshold: 133
  Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside
  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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear configure fragment</td>
<td>Clears the IP fragment reassembly configuration and resets the defaults.</td>
</tr>
<tr>
<td>clear fragment</td>
<td>Clears the operational data of the IP fragment reassembly module.</td>
</tr>
<tr>
<td>show running-config fragment</td>
<td>Displays the IP fragment reassembly configuration.</td>
</tr>
</tbody>
</table>
show gc

To display the garbage collection process statistics, use the `show gc` command.

```
show gc
```

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Examples

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

```
> 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear gc</td>
<td>Removes the garbage collection process statistics.</td>
</tr>
</tbody>
</table>
show h225

To display information for H.225 sessions established across the Firepower Threat Defense device, use the `show h225` command.

```plaintext
> 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
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 Firepower Threat Defense device 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 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.

### Usage Guidelines

The `show h225` command displays information for H.225 sessions established across the device.

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:

```
> 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
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show h245</td>
<td>Displays information for H.245 sessions established across the device by endpoints using slow start.</td>
</tr>
<tr>
<td>show h323 ras</td>
<td>Displays information for H.323 RAS sessions established across the device.</td>
</tr>
</tbody>
</table>
show h245

To display information for H.245 sessions established across the Firepower Threat Defense device by endpoints using slow start, use the show h245 command.

show h245

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The show h245 command displays information for H.245 sessions established across the Firepower Threat Defense device 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.)

Examples

The following is sample output from the show h245 command:

```
> show h245
Total: 1
   LOCAL   TPKT    FOREIGN   TPKT
   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 Firepower Threat Defense device. 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

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show h245</td>
<td>Displays information for H.245 sessions established across the Firepower Threat Defense device by endpoints using slow start.</td>
</tr>
<tr>
<td>Commands</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show h323 ras</td>
<td>Displays information for H.323 RAS sessions established across the Firepower Threat Defense device.</td>
</tr>
</tbody>
</table>
**show h323**

To display information for H.323 connections, use the `show h323` command.

```
show h323 {ras | gup}
```

**Syntax Description**

- **ras**
  
  Displays the H323 RAS sessions established across the Firepower Threat Defense device between a gatekeeper and its H.323 endpoint.

- **gup**
  
  Displays information about the H323 gateway updated protocol connections.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show h323 ras` command displays information for H.323 RAS sessions established across the Firepower Threat Defense device between a gatekeeper and its H.323 endpoint.

**Examples**

The following is sample output from the `show h323 ras` command:

```
> show h323 ras
Total: 1
          GK                      Caller
172.30.254.214  10.130.56.14
```

This output shows that there is one active registration between the gatekeeper 172.30.254.214 and its client 10.130.56.14.

**Related Commands**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show h245</td>
<td>Displays information for H.245 sessions established across the Firepower Threat Defense device by endpoints using slow start.</td>
</tr>
</tbody>
</table>
**show hardware-bypass**

To display the current hardware bypass status on an ISA 3000, use the `show hardware-bypass` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show hardware-bypass` command.

```plaintext
> show hardware-bypass

<table>
<thead>
<tr>
<th>Status</th>
<th>Powerdown</th>
<th>Powerup</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet 1/1-1/2</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>GigabitEthernet 1/3-1/4</td>
<td>Disable</td>
<td>Disable</td>
</tr>
</tbody>
</table>

Pairing supported on these interfaces: gig1/1 & gig1/2, gig1/3 & gig1/4
```
show high-availability config

To view information on the high-availability (failover) configuration, use the `show high-availability config` command.

**show high-availability config**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show high-availability config` command is an alias of the `show failover` command. For detailed information, see the reference page for `show failover`.

**Examples**

The following example shows the failover configuration for a device in Active/Standby failover mode.

```bash
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXJU, Mate 9A3MMFP0H1CP
  This host: Primary - Active
    Active time: 2009 (sec)
    slot 0: empty
    Interface diagnostic (0.0.0.0): Normal (Waiting)
    Interface outside (192.168.77.1): Normal (Waiting)
    Interface inside (192.168.87.1): Normal (Waiting)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)
  Other host: Secondary - Standby Ready
    Active time: 0 (sec)
    Interface diagnostic (0.0.0.0): Normal (Waiting)
    Interface outside (0.0.0.0): Normal (Waiting)
    Interface inside (0.0.0.0): Normal (Waiting)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics
Link : failover GigabitEthernet0/2 (up)
Stateful Obj xmit xerr rcv rerr
  General 235 0 234 0
  sys cmd 234 0 234 0
  up time 0 0 0 0
  RPC services 0 0 0 0
```
The following example shows what you see if the device is not currently configured for failover. The first line, which indicates that failover is off, is the only meaningful part of this output.

```plaintext
> show high-availability config
Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 12 of 160 maximum
MAC Address Move Notification Interval not set
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show failover</td>
<td>Shows the failover (high-availability) configuration.</td>
</tr>
</tbody>
</table>
show https-access-list

The `show https-access-list` command displays the HTTPS access lists configured on the device.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The HTTPS access list determines which addresses can make HTTPS connections to the management interface, the one configured with the `configure network ipv4/ipv6` commands. You use HTTPS connections to use the local manager, Firepower Device Manager, to configure and manage the device.

This access list does not control through-the-box traffic or HTTPS access to data interfaces.

### Examples

The following example shows the HTTPS access list for the management interface.

```
> show https-access-list
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:https
ACCEPT tcp anywhere anywhere state NEW tcp dpt:https
```

### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure</code> <code>https-access-list</code></td>
<td>Configures the HTTPS access list on the management interface.</td>
</tr>
</tbody>
</table>
show https-access-list
show i

- show idb, on page 573
- show igmp groups, on page 575
- show igmp interface, on page 576
- show igmp traffic, on page 577
- show inline-set, on page 578
- show interface, on page 579
- show interface ip brief, on page 590
- show inventory, on page 592
- show ip address, on page 595
- show ip address dhcp, on page 597
- show ip address pppoe, on page 601
- show ip audit count, on page 602
- show ip local pool, on page 603
- show ip verify statistics, on page 604
- show ipsec df-bit, on page 605
- show ipsec fragmentation, on page 606
- show ipsec policy, on page 607
- show ipsec sa, on page 608
- show ipsec sa summary, on page 617
- show ipsec stats, on page 618
- show ipv6 access-list, on page 622
- show ipv6 dhcp, on page 623
- show ipv6 dhcp relay binding, on page 628
- show ipv6 dhcp relay statistics, on page 629
- show ipv6 general-prefix, on page 630
- show ipv6 icmp, on page 631
- show ipv6 interface, on page 632
- show ipv6 local pool, on page 634
- show ipv6 mld traffic, on page 635
- show ipv6 neighbor, on page 636
- show ipv6 ospf, on page 638
- show ipv6 ospf border-routers, on page 639
- show ipv6 ospf database, on page 640
• show ipv6 ospf events, on page 643
• show ipv6 ospf flood-list, on page 645
• show ipv6 ospf graceful-restart, on page 646
• show ipv6 ospf interface, on page 647
• show ipv6 ospf request-list, on page 649
• show ipv6 ospf retransmission-list, on page 650
• show ipv6 ospf statistic, on page 651
• show ipv6 ospf summary-prefix, on page 652
• show ipv6 ospf timers, on page 653
• show ipv6 ospf traffic, on page 654
• show ipv6 ospf virtual-links, on page 655
• show ipv6 prefix-list, on page 656
• show ipv6 route, on page 658
• show ipv6 routers, on page 661
• show ipv6 traffic, on page 662
• show isakmp sa, on page 664
• show isakmp stats, on page 665
• show isis database, on page 667
• show isis hostname, on page 671
• show isis lsp-log, on page 672
• show isis neighbors, on page 674
• show isis rib, on page 676
• show isis spf-log, on page 678
• show isis topology, on page 681
**show idb**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

HWIDB# 1           0xdacf1420  Virtual0
HWIDB# 2           0xdac4da20  GigabitEthernet1/1
HWIDB# 3           0xdac5aa20  GigabitEthernet1/2
HWIDB# 4           0xdac651b0  GigabitEthernet1/3
HWIDB# 5           0xdac6f940  GigabitEthernet1/4
HWIDB# 6           0xdac7a0d0  GigabitEthernet1/5
HWIDB# 7           0xdac86f60  GigabitEthernet1/6
HWIDB# 8           0xdac8eff0  GigabitEthernet1/7
HWIDB# 9           0xdac97780  GigabitEthernet1/8
HWIDB# 10          0xdacbd00  Internal-Control1/1
HWIDB# 11          0xdaca3f10  Internal-Data1/1
HWIDB# 12          0xdacbb260  Internal-Data1/2
HWIDB# 13          0xdacc81a0  Internal-Data1/3
HWIDB# 14          0xdce0e4a0  Internal-Data1/4
HWIDB# 15          0xdce0d0d0  Management1/1

SWIDB# 1           0xdacfe840  Ox00000041 Virtual0 UP UP
SWIDB# 2           0xdadde40  Ox00000002 GigabitEthernet1/1 UP DOWN
SWIDB# 3           0xda95e40  Ox00000003 GigabitEthernet1/2 UP DOWN
SWIDB# 4           0xda55d0  0xffffffff GigabitEthernet1/3 DOWN DOWN
SWIDB# 5           0xda5f60  0xffffffff GigabitEthernet1/4 DOWN DOWN
SWIDB# 6           0xda7a4f0  0xffffffff GigabitEthernet1/5 DOWN DOWN
SWIDB# 7           0xda8c980  0xffffffff GigabitEthernet1/6 DOWN DOWN
SWIDB# 8           0xda8f410  0xffffffff GigabitEthernet1/7 DOWN DOWN
SWIDB# 9           0xda90ba0  0xffffffff GigabitEthernet1/8 DOWN DOWN
SWIDB# 10          0xda0bde20  Ox0000003f Internal-Control1/1 UP UP
SWIDB# 11          0xda84330  Ox00000043 Internal-Data1/1 UP UP
SWIDB# 12          0xda8c3680  Ox00000004 Internal-Data1/2 UP UP
SWIDB# 13          0xdaa85c0  Ox00000044 Internal-Data1/3 UP UP
SWIDB# 14          0xda82e210  Ox00000045 Internal-Data1/4 UP UP
SWIDB# 15          0xda49d0d0  Ox00000004 Management1/1 UP UP
```
The following table explains each field.

### Table 35: `show idb stats` Fields

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface</td>
<td>Displays the runtime status and statistics of interfaces.</td>
</tr>
</tbody>
</table>
show igmp groups

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

```
> show igmp groups

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp interface</td>
<td>Displays multicast information for an interface.</td>
</tr>
</tbody>
</table>
show igmp interface

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

```
show igmp interface [if_name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>if_name</code></td>
<td>(Optional) Displays IGMP group information for the selected interface.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show igmp groups</code></td>
<td>Displays the multicast groups with receivers that are directly connected to the Firepower Threat Defense device and that were learned through IGMP.</td>
</tr>
</tbody>
</table>
show igmp traffic

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

```
show igmp traffic
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear igmp counters</td>
<td>Clears all IGMP statistic counters.</td>
</tr>
<tr>
<td>clear igmp traffic</td>
<td>Clears the IGMP traffic counters.</td>
</tr>
</tbody>
</table>
show inline-set

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

```
show interface [ (physical_interface | redundant number) [ subinterface ] | interface_name | BVI id | ] [ summary | stats | detail ]
```

**Syntax Description**

- **BVI id**
  (Optional) Shows statistics for the indicated Bridge Virtual Interface (BVI). Enter the BVI number, from 1-250.

- **detail**
  (Optional) Shows detailed interface information, including the order in which the interface was added, the configured state, the actual state, and asymmetrical routing statistics, if enabled.

  If you show all interfaces, then you also see information about internal interfaces that are used for system communications. Internal interfaces are not user-configurable, and the information is for debugging purposes only.

- **interface_name**
  (Optional) Identifies the interface by logical name.

- **physical_interface**
  (Optional) Identifies the interface ID, such as `gigabitethernet0/1`. The available interfaces differ by device model. Use the show interface command without parameters to see the names available on your device.

- **redundant number**
  (Optional) Identifies the redundant interface ID, such as `redundant1`.

- **stats**
  (Default) Shows interface information and statistics. This keyword is the default, so this keyword is optional.

- **summary**
  (Optional) Shows summary information about an interface.

- **subinterface**
  (Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

**Command Default**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2</td>
<td>The <strong>BVI</strong> keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The number of statistics shown for subinterfaces is a subset of the number of statistics shown for a physical interface.
The number of bytes transmitted or received in the Hardware count and the Traffic Statistics count are different. In the hardware count, the amount is retrieved directly from hardware, and reflects the Layer 2 packet size. While in traffic statistics, it reflects the Layer 3 packet size. The count difference is varied based upon the design of the interface card hardware. For example, for a Fast Ethernet card, the Layer 2 count is 14 bytes greater than the traffic count, because it includes the Ethernet header. On the Gigabit Ethernet card, the Layer 2 count is 18 bytes greater than the traffic count, because it includes both the Ethernet header and the CRC. See the “Examples” section for a description of the display output.

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

```plaintext
> show interface
Interface GigabitEthernet1/1 "outside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex, Auto-Speed
  Input flow control is unsupported, output flow control is off
  MAC address e865.49b8.97f2, MTU 1500
  IP address unassigned
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  0 packets output, 0 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (2047/2047)
  output queue (blocks free curr/low): hardware (2047/2047)
Traffic Statistics for "outside":
  0 packets input, 0 bytes
  0 packets output, 0 bytes
  0 packets dropped
  1 minute input rate 0 pkts/sec, 0 bytes/sec
  1 minute output rate 0 pkts/sec, 0 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec, 0 bytes/sec
  5 minute output rate 0 pkts/sec, 0 bytes/sec
  5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/2 "inside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex, Auto-Speed
  Input flow control is unsupported, output flow control is off
  MAC address e865.49b8.97f3, MTU 1500
  IP address 192.168.45.1, subnet mask 255.255.255.0
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  0 packets output, 0 bytes, 0 underruns
```
Interface GigabitEthernet1/3 "", is administratively down, line protocol is down
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
Auto-Duplex, Auto-Speed
Input flow control is unsupported, output flow control is off
Available but not configured via nameif
MAC address e865.49b8.97f4, MTU not set
IP address unassigned
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runs, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
0 packets output, 0 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (2047/2047)
output queue (blocks free curr/low): hardware (2047/2047)

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

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

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

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

Interface GigabitEthernet1/8 
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
Auto-Duplex, Auto-Speed
Input flow control is unsupported, output flow control is off
Available but not configured via nameif
MAC address e865.49b8.97f9, MTU not set
IP address unassigned
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
0 packets output, 0 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (2047/2047)
output queue (blocks free curr/low): hardware (2047/2047)
Interface Management1/1 "diagnostic", is up, line protocol is up

Hardware is en_vtun rev00, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Pull-duplex), Auto-Speed(1000 Mbps)
Input flow control is unsupported, output flow control is off
MAC address e865.49b8.97f1, MTU 1500
IP address unassigned
14247681 packets input, 896591753 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
0 packets output, 0 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)

Traffic Statistics for "diagnostic":
14247685 packets input, 697121911 bytes
0 packets output, 0 bytes
5054964 packets dropped
1 minute input rate 2 pkts/sec, 131 bytes/sec
1 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute input rate 2 pkts/sec, 108 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
0 pause input, 0 resume input
0 L2 decode drops
Management-only interface. Blocked 0 through-the-device packets

The following table shows each field description.

**Table 36: show interface Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface ID</td>
<td>The interface ID.</td>
</tr>
<tr>
<td>&quot;interface_name&quot;</td>
<td>The logical interface name. If you do not configure a name, the following message appears after the Hardware line:</td>
</tr>
<tr>
<td>is state</td>
<td>The administrative state, as follows:</td>
</tr>
<tr>
<td></td>
<td>• up—The interface is not shut down.</td>
</tr>
<tr>
<td></td>
<td>• administratively down—The interface is shut down intentionally.</td>
</tr>
<tr>
<td>Line protocol is state</td>
<td>The line status, as follows:</td>
</tr>
<tr>
<td></td>
<td>• up—A working cable is plugged into the network interface.</td>
</tr>
<tr>
<td></td>
<td>• down—Either the cable is incorrect or not plugged into the interface connector.</td>
</tr>
<tr>
<td>VLAN identifier</td>
<td>For subinterfaces, the VLAN ID.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
Hardware | The interface type, maximum bandwidth, delay, duplex, and speed. When the link is down, the duplex and speed show the configured values. When the link is up, these fields show the configured values with the actual settings in parentheses.
Media-type | (Not always shown) Shows the interface media type, such as RJ-45 or SFP.
Message area | A message might be displayed in some circumstances. See the following examples:
- If you do not configure a name, you see the following message: Available but not configured via nameif
- If an interface is a member of a redundant interface, you see the following message: Active member of Redundant5
MAC address | The interface MAC address.
Site specific MAC address | For clustering, shows an in-use site-specific MAC address.
MTU | The maximum size, in bytes, of packets allowed on this interface. If you do not set the interface name, this field shows “MTU not set.”
IP address | The interface IP address, either static or received from a DHCP server.
Subnet mask | The subnet mask for the IP address.
Packets input | The number of packets received on this interface.
Bytes | The number of bytes received on this interface.
No buffer | The number of failures from block allocations.
Received: |
Broadcasts | The number of broadcasts received.
Input errors | The number of total input errors, including the types listed below. Other input-related errors can also cause the input error count to increase, and some datagrams might have more than one error; therefore, this sum might exceed the number of errors listed for the types below.
Runts | The number of packets that are discarded because they are smaller than the minimum packet size, which is 64 bytes. Runts are usually caused by collisions. They might also be caused by poor wiring and electrical interference.
Giants | The number of packets that are discarded because they exceed the maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRC</td>
<td>The number of Cyclical Redundancy Check errors. When a station sends a frame, it appends a CRC to the end of the frame. This CRC is generated from an algorithm based on the data in the frame. If the frame is altered between the source and destination, the system notes that the CRC does not match. A high number of CRCs is usually the result of collisions or a station transmitting bad data.</td>
</tr>
<tr>
<td>Frame</td>
<td>The number of frame errors. Bad frames include packets with an incorrect length or bad frame checksums. This error is usually the result of collisions or a malfunctioning Ethernet device.</td>
</tr>
<tr>
<td>Overrun</td>
<td>The number of times that the interface was incapable of handing received data to a hardware buffer because the input rate exceeded the interface’s capability to handle the data.</td>
</tr>
<tr>
<td>Ignored</td>
<td>This field is not used. The value is always 0.</td>
</tr>
<tr>
<td>Abort</td>
<td>This field is not used. The value is always 0.</td>
</tr>
<tr>
<td>L2 decode drops</td>
<td>The number of packets dropped because the name is not configured or a frame with an invalid VLAN id is received. On a standby interface in a redundant interface configuration, this counter may increase because this interface has no name configured.</td>
</tr>
<tr>
<td>Packets output</td>
<td>The number of packets sent on this interface.</td>
</tr>
<tr>
<td>Bytes</td>
<td>The number of bytes sent on this interface.</td>
</tr>
<tr>
<td>Underruns</td>
<td>The number of times that the transmitter ran faster than the interface could handle.</td>
</tr>
<tr>
<td>Output Errors</td>
<td>The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.</td>
</tr>
<tr>
<td>Collisions</td>
<td>The number of messages retransmitted due to an Ethernet collision (single and multiple collisions). This usually occurs on an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once by the output packets.</td>
</tr>
<tr>
<td>Interface resets</td>
<td>The number of times an interface has been reset. If an interface is unable to transmit for three seconds, the system resets the interface to restart transmission. During this interval, connection state is maintained. An interface reset can also happen when an interface is looped back or shut down.</td>
</tr>
<tr>
<td>Babbles</td>
<td>Unused. (&quot;babble&quot; means that the transmitter has been on the interface longer than the time taken to transmit the largest frame.)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Late collisions</td>
<td>The number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait. If you get a late collision, a device is jumping in and trying to send the packet on the Ethernet while the Firepower Threat Defense device is partly finished sending the packet. The Firepower Threat Defense device does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks and Ethernet networks running beyond the specification.</td>
</tr>
<tr>
<td>Deferred</td>
<td>The number of frames that were deferred before transmission due to activity on the link.</td>
</tr>
<tr>
<td>input reset drops</td>
<td>Counts the number of packets dropped in the RX ring when a reset occurs.</td>
</tr>
<tr>
<td>output reset drops</td>
<td>Counts the number of packets dropped in the TX ring when a reset occurs.</td>
</tr>
<tr>
<td>Rate limit drops</td>
<td>The number of packets dropped if you configured the interface at non-Gigabit speeds and attempted to transmit more than 10 Mbps or 100 Mbps, depending on configuration.</td>
</tr>
<tr>
<td>Lost carrier</td>
<td>The number of times the carrier signal was lost during transmission.</td>
</tr>
<tr>
<td>No carrier</td>
<td>Unused.</td>
</tr>
<tr>
<td>Input queue (curr/max packets):</td>
<td>The number of packets in the input queue, the current and the maximum.</td>
</tr>
<tr>
<td>Hardware</td>
<td>The number of packets in the hardware queue.</td>
</tr>
<tr>
<td>Software</td>
<td>The number of packets in the software queue. Not available for Gigabit Ethernet interfaces.</td>
</tr>
<tr>
<td>Output queue (curr/max packets):</td>
<td>The number of packets in the output queue, the current and the maximum.</td>
</tr>
<tr>
<td>Hardware</td>
<td>The number of packets in the hardware queue.</td>
</tr>
<tr>
<td>Software</td>
<td>The number of packets in the software queue.</td>
</tr>
<tr>
<td>input queue (blocks free curr/low)</td>
<td>The curr/low entry indicates the number of current and all-time-lowest available slots on the interface's Receive (input) descriptor ring. These are updated by the main CPU, so the all-time-lowest (until the interface statistics are cleared or the device is reloaded) watermarks are not highly accurate.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>output queue (blocks free curr/low)</td>
<td>The curr/low entry indicates the number of current and all-time-lowest available slots on the interface's Transmit (output) descriptor rings. These are updated by the main CPU, so the all-time-lowest (until the interface statistics are cleared or the device is reloaded) watermarks are not highly accurate.</td>
</tr>
</tbody>
</table>

**Traffic Statistics:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets input</td>
<td>The number of packets received and the number of bytes.</td>
</tr>
<tr>
<td>Packets output</td>
<td>The number of packets transmitted and the number of bytes.</td>
</tr>
</tbody>
</table>
| Packets dropped | The number of packets dropped. Typically this counter increments for packets dropped on the accelerated security path (ASP), for example, if a packet is dropped due to an access list deny.  
See the `show asp drop` command for reasons for potential drops on an interface. |

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 minute input rate</td>
<td>The number of packets received in packets/sec and bytes/sec over the last minute.</td>
</tr>
<tr>
<td>1 minute output rate</td>
<td>The number of packets transmitted in packets/sec and bytes/sec over the last minute.</td>
</tr>
<tr>
<td>1 minute drop rate</td>
<td>The number of packets dropped in packets/sec over the last minute.</td>
</tr>
<tr>
<td>5 minute input rate</td>
<td>The number of packets received in packets/sec and bytes/sec over the last 5 minutes.</td>
</tr>
<tr>
<td>5 minute output rate</td>
<td>The number of packets transmitted in packets/sec and bytes/sec over the last 5 minutes.</td>
</tr>
<tr>
<td>5 minute drop rate</td>
<td>The number of packets dropped in packets/sec over the last 5 minutes.</td>
</tr>
</tbody>
</table>

**Redundancy Information:**

For redundant interfaces, shows the member physical interfaces. The active interface has “(Active)” after the interface ID.  
If you have not yet assigned members, you see the following output:  

| Members unassigned |

For redundant interfaces, shows the last time the active interface failed over to the standby interface.

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

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

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

**Table 37: show interface detail Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demux drops</td>
<td>(On Internal-Data interface only) The number of packets dropped because the Firepower Threat Defense device was unable to demultiplex packets from other interfaces.</td>
</tr>
<tr>
<td>Control Point Interface States:</td>
<td></td>
</tr>
<tr>
<td>Interface number</td>
<td>A number used for debugging that indicates in what order this interface was created, starting with 0.</td>
</tr>
</tbody>
</table>
| Interface config status | The administrative state, as follows:  
  • active—The interface is not shut down.  
  • not active—The interface is shut down intentionally. |
### Interface state
The actual state of the interface. In most cases, this state matches the config status above. If you configure high availability, it is possible there can be a mismatch because the Firepower Threat Defense device brings the interfaces up or down as needed.

### Asymmetrical Routing Statistics:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received X1 packets</td>
<td>Number of ASR packets received on this interface.</td>
</tr>
<tr>
<td>Transmitted X2 packets</td>
<td>Number of ASR packets sent on this interface.</td>
</tr>
<tr>
<td>Dropped X3 packets</td>
<td>Number of ASR packets dropped on this interface. The packets might be dropped if the interface is down when trying to forward the packet.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear interface</td>
<td>Clears counters for the show interface command.</td>
</tr>
<tr>
<td>show interface ip brief</td>
<td>Shows the interface IP address and status.</td>
</tr>
</tbody>
</table>
show interface ip brief

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

```
show interface [ [physical_interface [,subinterface] | interface_name | BVI id ] ] ip brief
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BVI id</td>
<td>(Optional) Shows statistics for the indicated Bridge Virtual Interface (BVI). Enter the BVI number, from 1-250.</td>
</tr>
<tr>
<td>interface_name</td>
<td>(Optional) Identifies the interface name.</td>
</tr>
<tr>
<td>physical_interface</td>
<td>(Optional) Identifies the interface ID, such as <code>gigabitethernet0/1</code>.</td>
</tr>
<tr>
<td>subinterface</td>
<td>(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.</td>
</tr>
</tbody>
</table>

**Command Default**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2</td>
<td>The BVI keyword was added.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show interface ip brief

Interface          | IP-Address | OK? Method | Status          | Protocol         |
Control0/0          | 127.0.0.1.1| YES CONFIG | up              | up               |
GigabitEthernet0/0  | 209.165.200.226| YES CONFIG | up              | up               |
GigabitEthernet0/1  | unassigned | YES unset  | administratively down | down           |
GigabitEthernet0/2  | 10.1.1.50  | YES manual | administratively down | down           |
GigabitEthernet0/3  | 192.168.2.6 | YES DHCP   | administratively down | down           |
Management0/0        | 209.165.201.3| YES CONFIG | up              | up               |

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

```
> show interface ip brief

| Interface           | IP-Address | OK? Method | Status          | Protocol |
GigabitEthernet1/1   | unassigned | YES DHCP   | down            | down     |
GigabitEthernet1/2   | 192.168.1.1 | YES unset  | down            | down     |
GigabitEthernet1/3   | 192.168.1.1 | YES unset  | down            | down     |
GigabitEthernet1/4   | 192.168.1.1 | YES unset  | down            | down     |
GigabitEthernet1/5   | 192.168.1.1 | YES unset  | down            | down     |
GigabitEthernet1/6   | 192.168.1.1 | YES unset  | down            | down     |
GigabitEthernet1/7   | 192.168.1.1 | YES unset  | down            | down     |
GigabitEthernet1/8   | 192.168.1.1 | YES unset  | down            | down     |
Internal-Control1/1  | 127.0.0.1.1 | YES unset  | up              | up       |
Internal-Data1/1     | unassigned | YES unset  | up              | up       |
```
The following table explains the output fields.

### Table 38: show interface ip brief Fields

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface</td>
<td>Displays the runtime status and statistics of interfaces.</td>
</tr>
</tbody>
</table>
show inventory

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

```
show inventory [slot_id]
```

**Syntax Description**

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

**Command Default**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

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

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

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

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

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

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

Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A , VID: N/A, SN: N/A

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

Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"

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

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

Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"

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

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

Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"

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

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

Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"

PID: ASA-IC-6GE-CU-B , VID: N/A, SN: N/A

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

Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"

PID: ASA-IC-6GE-CU-C , VID: N/A, SN: N/A

Examples

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

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

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

The following table describes the fields shown in the display.

Table 39: Field Descriptions for show inventory

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Physical name (text string) assigned to the Cisco entity. For example, console, SSP, or a simple component number (port or module number), such as &quot;1,&quot; depending on the physical component naming syntax of the device. Equivalent to the entPhysicalName MIB variable in RFC 2737.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>DESCR</td>
<td>Physical description of the Cisco entity that characterizes the object. Equivalent to the entPhysicalDesc MIB variable in RFC 2737.</td>
</tr>
<tr>
<td>PID</td>
<td>Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.</td>
</tr>
<tr>
<td>VID</td>
<td>Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.</td>
</tr>
<tr>
<td>SN</td>
<td>Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.</td>
</tr>
</tbody>
</table>
show ip address

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface_name</code></td>
<td>(Optional) Identifies the interface name.</td>
</tr>
<tr>
<td><code>physical_interface</code></td>
<td>(Optional) Identifies the interface ID, such as <code>gigabitethernet0/1</code>.</td>
</tr>
<tr>
<td><code>subinterface</code></td>
<td>(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.</td>
</tr>
</tbody>
</table>

**Command Default**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

**Examples**

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

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

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

The following table explains each field.
Table 40: show ip address Fields

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface</td>
<td>Displays the runtime status and statistics of interfaces.</td>
</tr>
<tr>
<td>show interface ip brief</td>
<td>Shows the interface IP address and status.</td>
</tr>
</tbody>
</table>
show ip address dhcp

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface_name</code></td>
<td>Identifies the interface name.</td>
</tr>
<tr>
<td><code>lease</code></td>
<td>Shows information about the DHCP lease.</td>
</tr>
<tr>
<td><code>physical_interface</code></td>
<td>Identifies the interface ID, such as <code>gigabitethernet0/1</code>.</td>
</tr>
<tr>
<td><code>proxy</code></td>
<td>Shows proxy entries in the IPL table.</td>
</tr>
<tr>
<td><code>server</code></td>
<td>Shows server entries in the IPL table.</td>
</tr>
<tr>
<td><code>subinterface</code></td>
<td>Identifies an integer between 1 and 4294967293 designating a logical subinterface.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>Shows summary for the entry.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

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

The following table explains each field.

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

The client ID used in all communication with the server.

Specifies if this interface is a proxy DHCP client for VPN clients, True or False.

The requested network.

The client hostname.

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

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

DHCP server: 40.7.12.6
Leases: 1
Offers: 1 Requests: 17 Acks: 17 Naks: 0
Declines: 0 Releases: 0 Bad: 0
DNS0: 171.69.160.23, DNS1: 171.69.160.24
WINS0: 172.69.160.23, WINS1: 172.69.160.23
Subnet: 255.255.0.0 DNS Domain: cisco.com
```

The following table explains each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server</td>
<td>The DHCP server address from which this interface obtained a lease. The top entry (“ANY”) is the default server and is always present.</td>
</tr>
<tr>
<td>Leases</td>
<td>The number of leases obtained from the server. For an interface, the number of leases is typically 1. If the server is providing address for an interface that is running proxy for VPN, there will be several leases.</td>
</tr>
<tr>
<td>Offers</td>
<td>The number of offers from the server.</td>
</tr>
<tr>
<td>Requests</td>
<td>The number of requests sent to the server.</td>
</tr>
<tr>
<td>Ack</td>
<td>The number of acknowledgments received from the server.</td>
</tr>
<tr>
<td>Naks</td>
<td>The number of negative acknowledgments received from the server.</td>
</tr>
<tr>
<td>Declines</td>
<td>The number of declines received from the server.</td>
</tr>
<tr>
<td>Releases</td>
<td>The number of releases sent to the server.</td>
</tr>
</tbody>
</table>
Field | Description
---|---
Bad | The number of bad packets received from the server.
DNS0 | The primary DNS server address obtained from the DHCP server.
DNS1 | The secondary DNS server address obtained from the DHCP server.
WINS0 | The primary WINS server address obtained from the DHCP server.
WINS1 | The secondary WINS server address obtained from the DHCP server.
Subnet | The subnet address obtained from the DHCP server.
DNS Domain | The domain obtained from the DHCP server.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interface ip brief</code></td>
<td>Shows the interface IP address and status.</td>
</tr>
<tr>
<td><code>show ip address</code></td>
<td>Displays the IP addresses of interfaces.</td>
</tr>
</tbody>
</table>
show ip address pppoe

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface_name</code></td>
<td>Identifies the interface name.</td>
</tr>
<tr>
<td><code>physical_interface</code></td>
<td>Identifies the interface ID, such as <code>gigabitethernet0/1</code>.</td>
</tr>
<tr>
<td><code>subinterface</code></td>
<td>Identifies an integer between 1 and 4294967293 designating a logical subinterface.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interface ip brief</code></td>
<td>Shows the interface IP address and status.</td>
</tr>
<tr>
<td><code>show ip address</code></td>
<td>Displays the IP addresses of interfaces.</td>
</tr>
</tbody>
</table>
show ip audit count

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip audit count</td>
<td>Clears the statistics for IP audit.</td>
</tr>
<tr>
<td>show running-config ip audit name</td>
<td>Shows the configuration for the <code>ip audit name</code> command. Besides <code>name</code>, you can check on the <code>interface</code> and <code>signature</code> configuration.</td>
</tr>
</tbody>
</table>
show ip local pool

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

```
show ip local pool pool_name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool_name</td>
<td>The name of an IPv6 address pool.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

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

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

```bash
show ip verify statistics [ interface  interface_name ]
```

### Syntax Description

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

### Command Default

This command shows statistics for all interfaces.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

### Examples

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip verify statistics</td>
<td>Clears the Unicast RPF statistics.</td>
</tr>
<tr>
<td>show running-config ip verify reverse-path</td>
<td>Shows the <strong>ip verify reverse-path</strong> configuration.</td>
</tr>
</tbody>
</table>
**show ipsec df-bit**

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

`show ipsec df-bit interface`

**Syntax Description**

| interface | Specifies an interface name. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipsec fragmentation</code></td>
<td>Displays the fragmentation policy for IPsec packets.</td>
</tr>
</tbody>
</table>
show ipsec fragmentation

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

`show ipsec fragmentation` interface

**Syntax Description**

- **interface**
  
  Specifies an interface name.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipsec df-bit</td>
<td>Displays the DF-bit policy for a specified interface.</td>
</tr>
</tbody>
</table>
show ipsec policy

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

show ipsec policy

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example shows the OSPFv3 authentication and encryption policy.

```
> show ipsec policy
Crypto IPsec client security policy data
Policy name: OSPFv3-1-256
Policy refcount: 1
Policy flags: 0x00000000
SA handles: sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound ESP SPI: 256 (0x100)
Outbound ESP SPI: 256 (0x100)
Inbound ESP Auth Key: 1234567890123456789012345678901234567890
Outbound ESP Auth Key: 1234567890123456789012345678901234567890
Inbound ESP Cipher Key: 1234567890123456789012345678901234567890
Outbound ESP Cipher Key: 1234567890123456789012345678901234567890
Transform set: esp-aes esp-sha-hmac
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show crypto sockets</td>
<td>Displays secure socket information.</td>
</tr>
<tr>
<td>show ipv6 ospf interface</td>
<td>Displays information about OSPFv3 interfaces.</td>
</tr>
</tbody>
</table>
show ipsec sa

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23
    local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
    remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
    current_peer: 75.2.1.60, username: rashmi
    dynamic allocated peer ip: 65.2.1.100
    dynamic allocated peer ip(ipv6): 2001:1000::10
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
    #FMTUs sent: 0, #FMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```
The following example displays IPsec SAs, including an in-use setting to identify a tunnel as OSPFv3.

```plaintext
> 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)
    currentpeer: 172.20.0.21
    dynamic allocated peer ip: 10.135.1.5
    #pktsencaps: 0, #pktsencrypt: 0, #pktsdigest: 0
    #pktsdecaps: 1145, #pktsdecrypt: 1145, #pktsverify: 1145
    #pktscompressed: 0, #pktsdecompressed: 0
    #pktsnotcompressed: 0, #pktscompfailed: 0, #pktsdecompfailed: 0
    #pre-fragsuccesses: 2, #pre-fragfailures: 1, #fragmentscreated: 10
    #PMTUs sent: 5, #PMTUs rcvd: 2, #decapulatedfragsnedingreassemble: 1
    #senderrors: 0, #recverrors: 0
    local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21
    pathmtu1500, ipsec overhead 60, media mtu 1500
    current outbound spi: DC15BF68
inbound esp sas:
  spi: 0x1E8246FC2 (511854332)
    transform: esp-3des esp-md5-hmac
    in use settings = {L2L, Transport, Manual key (OSPFv3),}
    slot: 0, conn_id: 3, crypto-map: def
    sa timing: remaining key lifetime (sec): 548
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x00000001
outbound esp sas:
  spi: 0x702246FC (1338730020)
    transform: esp-3des esp-sha-hmac no compression
    in use settings = {RA, Transport, NAT-T-Encaps, GRE, IKEv2,}
    slot: 0, conn_id: 192, crypto-map: def
    sa timing: remaining key lifetime (sec): 28387
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x0003FFFF 0xFFFFFFFF
```
spi: 0xDC15BF68 (3692412776)
   transform: esp-3des esp-md5-hmac
   in use settings ={L2L, Transport, Manual key (OSPFv3), }
   slot: 0, conn_id: 3, crypto-map: def
   sa timing: remaining key lifetime (sec): 548
   IV size: 8 bytes
   replay detection support: Y

Crypto map tag: def, local addr: 10.132.0.17
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

---

**Note**

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

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

```bash
> 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
```
The following example shows IPsec SAs for the keyword entry.

```plaintext
> 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
```

```plaintext
> show ipsec sa
```
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): (192.168.132.0/255.255.255.255/0/0)
current_peer: 10.135.1.8
dynamic allocated peer ip: 0.0.0.0
#pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
#pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0
local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 3B6F6A35

inbound esp sas:
spi: 0xB32CF0BD (3006066877)
  transform: esp-3des esp-md5-hmac
  in use settings = {RA, Tunnel, }
  slot: 0, conn_id: 4, crypto-map: def
  sa timing: remaining key lifetime (sec): 212
  IV size: 8 bytes
  replay detection support: Y
outbound esp sas:
spi: 0x3B6F6A35 (997157429)
  transform: esp-3des esp-md5-hmac
  in use settings = {RA, Tunnel, }
  slot: 0, conn_id: 4, crypto-map: def
  sa timing: remaining key lifetime (sec): 212
  IV size: 8 bytes
  replay detection support: Y
The following example shows IPsec SAs with the keywords entry detail.

> show ipsec sa entry detail
peer address: 10.132.0.21
Crypto map tag: def, local addr: 172.20.0.17
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
current_peer: 10.132.0.21
dynamic allocated peer ip: 90.135.1.5
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
# pkts replay rollover (send): 0, # pkts replay rollover (rcv): 0
# pkts replay failed (rcv): 0
# pkts internal err (send): 0, # pkts internal err (rcv): 0

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

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

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

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

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

  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 invalid prot (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: 386F6A35

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: 0x386F6A35 (997157429)
  transform: esp-3des esp-md5-hmac
  in use settings = {RA, Tunnel, }
  slot: 0, conn_id: 4, crypto-map: def
**show ipsec sa**

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

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

```plaintext
> 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 not compressed: 0, #pkts comp failed: 0, #pkts decompress 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 decompress 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**.

```plaintext
> 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 decompress failed: 0
    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
```
The following example displays IPSec SAs based on IPv6 assigned address:

```plaintext
> show ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
Crypto map tag: def, seq num: 1, local addr: 75.2.1.23
local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
current_peer: 75.2.1.60, username: rashmi
dynamic allocated peer ip: 65.2.1.100
dynamic allocated peer ip(ipv6): 2001:1000::10
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pkts post-frag successes: 0, #pkts post-frag failures: 0, #fragments created: 0
#decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 35
local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
path mtu 1342, ipsec overhead 62 (44), override mtu 1280, media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
```
current inbound spi : 4FCB6624

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

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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isakmp sa</td>
<td></td>
<td>Clears the IKE runtime SA database.</td>
</tr>
<tr>
<td>show running-config isakmp</td>
<td></td>
<td>Displays all the active ISAKMP configuration.</td>
</tr>
</tbody>
</table>
show ipsec sa summary

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

**show ipsec sa summary**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipsec sa</td>
<td>Removes IPsec SAs entirely or based on specific parameters.</td>
</tr>
<tr>
<td>show ipsec sa</td>
<td>Displays a list of IPsec SAs.</td>
</tr>
<tr>
<td>show ipsec stats</td>
<td>Displays a list of IPsec statistics.</td>
</tr>
</tbody>
</table>
show ipsec stats

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

**show ipsec stats**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The following table describes what the output entries indicate.

<table>
<thead>
<tr>
<th>Output (continued)</th>
<th>Description (continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec Global Statistics</td>
<td>This section pertains to the total number of IPsec tunnels that the Firepower Threat Defense device supports.</td>
</tr>
<tr>
<td>Active tunnels</td>
<td>The number of IPsec tunnels that are currently connected.</td>
</tr>
<tr>
<td>Previous tunnels</td>
<td>The number of IPsec tunnels that have been connected, including the active ones.</td>
</tr>
<tr>
<td>Inbound</td>
<td>This section pertains to inbound encrypted traffic that is received through IPsec tunnels.</td>
</tr>
<tr>
<td>Bytes</td>
<td>The number of bytes of encrypted traffic that has been received.</td>
</tr>
<tr>
<td>Decompressed bytes</td>
<td>The number of bytes of encrypted traffic that were received after decompression was performed, if applicable. This counter should always be equal to the previous one if compression is not enabled.</td>
</tr>
<tr>
<td>Packets</td>
<td>The number of encrypted IPsec packets that were received.</td>
</tr>
<tr>
<td>Dropped packets</td>
<td>The number of encrypted IPsec packets that were received and dropped because of errors.</td>
</tr>
<tr>
<td>Replay failures</td>
<td>The number of anti-replay failure that were detected on received, encrypted IPsec packets.</td>
</tr>
<tr>
<td>Authenticizations</td>
<td>The number of successful authentications performed on received, encrypted IPsec packets.</td>
</tr>
<tr>
<td>Authentication failures</td>
<td>The number of authentications failure detected on received, encrypted IPsec packets.</td>
</tr>
<tr>
<td>Decryptions</td>
<td>The number of successful decryptions performed on received, encrypted IPsec packets.</td>
</tr>
<tr>
<td>Decryption failures</td>
<td>The number of decryptions failures detected on received, encrypted IPsec packets.</td>
</tr>
<tr>
<td><strong>Output (continued)</strong></td>
<td><strong>Description (continued)</strong></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Decapsulated fragments needing reassembly</td>
<td>The number of decryption IPsec packets that include IP fragments to be reassembled.</td>
</tr>
<tr>
<td>Outbound</td>
<td>This section pertains to outbound cleartext traffic to be transmitted through IPsec traffic.</td>
</tr>
<tr>
<td>Bytes</td>
<td>The number of bytes of cleartext traffic to be encrypted and transmitted through IPsec tunnels.</td>
</tr>
<tr>
<td>Uncompressed bytes</td>
<td>The number of bytes of uncompressed cleartext traffic to be encrypted and transmitted through IPsec tunnels. The counter should always be equal to the previous one if compression is not enabled</td>
</tr>
<tr>
<td>Packets</td>
<td>The number of cleartext packets to be encrypted and transmitted through IPsec tunnels.</td>
</tr>
<tr>
<td>Dropped packets</td>
<td>The number of cleartext packets to be encrypted and transmitted through IPsec tunnels that have been dropped because of errors.</td>
</tr>
<tr>
<td>Authentications</td>
<td>The number of successful authentications performed on packets to be transmitted through IPsec tunnels.</td>
</tr>
<tr>
<td>Authentication failures</td>
<td>The number of authentication failures that were detected on packets to be transmitted through IPsec tunnels.</td>
</tr>
<tr>
<td>Encryptions</td>
<td>The number of successful encryptions that were performed on packets to be transmitted through IPsec tunnels.</td>
</tr>
<tr>
<td>Encryption failures</td>
<td>The number of encryption failures that were detected on packets to be transmitted through IPsec tunnels.</td>
</tr>
<tr>
<td>Fragmentation successes</td>
<td>The number of successful fragmentation operations that were performed as part of outbound IPsec packet transformation.</td>
</tr>
<tr>
<td>Pre-fragmentation successes</td>
<td>The number of successful prefragmentation operations that were performed as part of outbound IPsec packet transformation. Prefragmentation occurs before the cleartext packet is encrypted and encapsulated as one or more IPsec packets.</td>
</tr>
<tr>
<td>Post-fragmentation successes</td>
<td>The number of successful prefragmentation operations that were performed as part of outbound IPsec packet transformation. Post-fragmentation occurs after the cleartext packet is encrypted and encapsulated as an IPsec packet, which results in multiple IP fragments. These fragments must be reassembled before decryption.</td>
</tr>
<tr>
<td>Fragmentation failures</td>
<td>The number of fragmentation failures that have occurred during outbound IPsec packet transformation.</td>
</tr>
<tr>
<td>Pre-fragmentation failures</td>
<td>The number of prefragmentation failures that have occurred during outbound IPsec packet transformation. Prefragmentation occurs before the cleartext packet is encrypted and encapsulated as one or more IPsec packets.</td>
</tr>
</tbody>
</table>
The number of post-fragmentation failure that have occurred during outbound IPsec packet transformation. Post-fragmentation occurs after the cleartext packet is encrypted and encapsulated as an IPsec packet, which results in multiple IP fragments. These fragments must be reassembled before decryption.

Fragments created

The number of fragments that were created as part of IPsec transformation.

PMTUs sent

The number of path MTU messages that were sent by the IPsec system. IPsec will send a PMTU message to an inside host that is sending packets that are too large to be transmitted through an IPsec tunnel after encapsulation. The PMTU message is a request for the host to lower its MTU and send smaller packets for transmission through the IPsec tunnel.

PMTUs rcvd

The number of path MTU messages that were received by the IPsec system. IPsec will receive a path MTU message from a downstream network element if the packets it is sending through the tunnel are too large to traverse that network element. IPsec will usually lower its tunnel MTU when a path MTU message is received.

Protocol failures

The number of malformed IPsec packets that have been received.

Missing SA failures

The number of IPsec operations that have been requested for which the specified IPsec security association does not exist.

System capacity failures

The number of IPsec operations that cannot be completed because the capacity of the IPsec system is not high enough to support the data rate.

Examples

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

```bash
> show ipsec stats

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipsec sa</td>
<td>Clears IPsec SAs or counters based on specified parameters.</td>
</tr>
<tr>
<td>show ipsec sa</td>
<td>Displays IPsec SAs based on specified parameters.</td>
</tr>
<tr>
<td>show ipsec sa summary</td>
<td>Displays a summary of IPsec SAs.</td>
</tr>
</tbody>
</table>
show ipv6 access-list

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

- show access-list
- show access-control-config
show ipv6 dhcp

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>client [pd] statistics</td>
<td>Shows DHCPv6 client statistics and shows the output of the number of messages sent and received. Add the pd keyword to show DHCPv6 Prefix Delegation client statistics.</td>
</tr>
<tr>
<td>interface [interface_name [statistics]]</td>
<td>Shows DHCPv6 information for all interfaces, or optionally, the specified interface. If the interface is configured for DHCPv6 stateless server configuration, this command lists the DHCPv6 pool that is being used by the server. If the interface has DHCPv6 address client or Prefix Delegation client configuration, this command shows the state of each client and the values received from the server.</td>
</tr>
<tr>
<td>ha statistics</td>
<td>Shows the transaction statistics between failover units, including how many times the DUID information was synced between the units.</td>
</tr>
<tr>
<td>server statistics</td>
<td>Shows the DHCPv6 stateless server statistics.</td>
</tr>
<tr>
<td>pool [pool_name]</td>
<td>Shows all DHCPv6 pools or optionally, the specified pool.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you do not specify any arguments, this command displays the device DUID that is being used by the DHCPv6 client or server.</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

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

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

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

```
> show ipv6 dhcp pool
DHCPv6 pool: Sample-Pool
Imported DNS server: 2004:abcd:abcd:abcd::2
Imported DNS server: 2004:abcd:abcd:abcd::4
Imported Domain name: relay.com
Imported Domain name: server.com
```
SIP server address: 2001::abcd:1
SIP server domain name: sip.xyz.com

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

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

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47

List of known servers:
  Reachable via address: fe80::20c:29ff:fe96:1bf4
  DUID: 000100011D9D1712005056A07E06
  Preference: 0
  Configuration parameters:
    IA PD: IA ID 0x00030001, T1 250, T2 400
      Prefix: 2005:abcd:ab03::/48
        preferred lifetime 500, valid lifetime 600
        expires at Nov 26 2014 03:11 PM (577 seconds)
    IA NA: IA ID 0x00030001, T1 250, T2 400
        preferred lifetime 500, valid lifetime 600
        expires at Nov 26 2014 03:11 PM (577 seconds)
  DNS server: 2004:abcd:abcd:abcd::2
  DNS server: 2004:abcd:abcd:abcd::4
  Domain name: relay.com
  Domain name: server.com
  Information refresh time: 0

Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44

List of known servers:
  Reachable via address: fe80::4e00:82ff:fe6f:916f
  DUID: 000300014C00826FF6F8
  Preference: 0
  Configuration parameters:
    IA NA: IA ID 0x000a0001, T1 43200, T2 69120
      Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
        preferred lifetime INFINITY, valid lifetime INFINITY
  Information refresh time: 0

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

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

Prefix State is OPEN
Renew will be sent in 00:02:05
Address State is OPEN
Renew for address will be sent in 00:02:06
List of known servers:
  Reachable via address: fe80::20c:29ff:fe96:1bf4
  DUID: 000100011D9D1712005056A07E06
```
Preference: 0

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

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

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

Protocol Exchange Statistics:

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

Error and Failure Statistics:

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

DHCPV6 Client address statistics:

Protocol Exchange Statistics:

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

Error and Failure Statistics:

  Number of Re-transmission messages sent: 1
  Number of Message Validation errors in received messages: 0
```
The following is sample output from the `show ipv6 dhcp client statistics` command:

```
> show ipv6 dhcp client statistics
Protocol Exchange Statistics:
  Total number of Solicit messages sent: 4
  Total number of Advertise messages received: 4
  Total number of Request messages sent: 4
  Total number of Renew messages sent: 92
  Total number of Rebind messages sent: 0
  Total number of Reply messages received: 96
  Total number of Release messages sent: 6
  Total number of Reconfigure messages received: 0
  Total number of Information-request messages sent: 0

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

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

```
> show ipv6 dhcp client pd statistics
Protocol Exchange Statistics:
  Total number of Solicit messages sent: 1
  Total number of Advertise messages received: 1
  Total number of Request messages sent: 1
  Total number of Renew messages sent: 92
  Total number of Rebind messages sent: 0
  Total number of Reply messages received: 93
  Total number of Release messages sent: 0
  Total number of Reconfigure messages received: 0
  Total number of Information-request messages sent: 0

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

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

```
> show ipv6 dhcp server statistics
Protocol Exchange Statistics:
  Total number of Solicit messages received: 0
  Total number of Advertise messages sent: 0
  Total number of Request messages received: 0
  Total number of Renew messages received: 0
  Total number of Rebind messages received: 0
  Total number of Reply messages sent: 10
  Total number of Release messages received: 0
  Total number of Reconfigure messages sent: 0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received: 0
  Total number of Relay-Reply messages sent: 0

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

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

```plaintext
> show ipv6 dhcp ha statistics

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

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

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

```plaintext
> show ipv6 dhcp ha statistics

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 dhcp</td>
<td>Clears the DHCPv6 statistics.</td>
</tr>
</tbody>
</table>
show ipv6 dhcprelay binding

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

```
> show ipv6 dhcprelay binding
1 in use, 2 most used
Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 dhcprelay</td>
<td>Shows the IPv6 DHCP relay agent information.</td>
</tr>
<tr>
<td>statistics</td>
<td></td>
</tr>
</tbody>
</table>
**show ipv6 dhcprelay statistics**

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

**show ipv6 dhcprelay statistics**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

Total Relay Bindings Created: 498
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 dhcprelay binding</td>
<td>Shows the relay binding entries created by the relay agent.</td>
</tr>
</tbody>
</table>
show ipv6 general-prefix

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

```
show ipv6 general-prefix
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

```
> show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
Loopback42 (Address command)
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default  N - Not advertised, C - Calendar
AD   fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```
show ipv6 icmp

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

```
show ipv6 icmp
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

### Examples

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

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

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

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

**Syntax Description**

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

**Command Default**

Displays all IPv6 interfaces.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

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

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

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

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

AD      fec0::0::a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```
show ipv6 local pool

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

```
show ipv6 local pool pool_name
```

**Syntax Description**

| pool_name | The name of an IPv6 address pool. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

Available Addresses:
2001:db8::db8:800:200c:417a
2001:db8::db8:800:200c:417b
2001:db8::db8:800:200c:417c
2001:db8::db8:800:200c:417d
2001:db8::db8:800:200c:417e
2001:db8::db8:800:200c:417f
2001:db8::db8:800:200c:4180
2001:db8::db8:800:200c:4181
2001:db8::db8:800:200c:4182
2001:db8::db8:800:200c:4183
2001:db8::db8:800:200c:4184
2001:db8::db8:800:200c:4185
2001:db8::db8:800:200c:4186
2001:db8::db8:800:200c:4187
2001:db8::db8:800:200c:4188
```
show ipv6 mld traffic

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

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

### Examples

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 mld traffic</td>
<td>Resets all MLD traffic counters.</td>
</tr>
</tbody>
</table>
show ipv6 neighbor

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

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

**Syntax Description**

- `address` (Optional) Displays neighbor discovery cache information for the supplied IPv6 address only.
- `if_name` (Optional) Displays cache information for the supplied interface name.

If you show all interfaces, then you also see information about internal interfaces that are used for system communications. Internal interfaces are not user-configurable, and the information is for debugging purposes only.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

**Note**

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

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

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

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

- ???—Unknown state.

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

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

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

- Interface

  The interface from which the address was reachable.

Examples

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

```bash
> show ipv6 neighbor inside
IPv6 Address Age Link-layer Addr State Interface
2000:0:0::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:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 neighbors</td>
<td>Deletes all entries in the IPv6 neighbor discovery cache, except static entries.</td>
</tr>
</tbody>
</table>
**show ipv6 ospf**

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

```
show ipv6 ospf [process_id] [area_id]
```

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 ospf border-routers</code></td>
<td>Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
<tr>
<td><code>show ipv6 ospf database</code></td>
<td>Shows lists of information related to the OSPFv3 database for a specific router.</td>
</tr>
</tbody>
</table>
**show ipv6 ospf border-routers**

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>process_id</code></td>
<td>(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPFv3 routing process is enabled.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

**Examples**

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

```
> show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 ospf</code></td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
<tr>
<td><code>show ipv6 ospf database</code></td>
<td>Shows lists of information related to the OSPFv3 database for a specific router.</td>
</tr>
</tbody>
</table>
show ipv6 ospf database

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

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

### Syntax Description

- **adv-router router-id**: (Optional) Displays all the LSAs of the advertising router. The router ID must be in the form documented in RFC 2740, in which the address is specified in hexadecimal using 16-bit values between colons.

- **area**: (Optional) Displays information only about area LSAs.

- **area_id**: (Optional) Displays information about a specified area only.

- **as**: (Optional) Filters unknown autonomous system (AS) LSAs.

- **database-summary**: (Optional) Displays how many of each type of LSA exists for each area in the database and the total.

- **destination-router-id**: (Optional) Displays information about a specified destination router only.

- **external**: (Optional) Displays information only about the external LSAs.

- **interface**: Optional) Displays information about the LSAs filtered by interface context.

- **interface-name**: (Optional) Specifies the LSA interface name.

- **internal**: (Optional) Displays information only about the internal LSAs.

- **inter-area prefix**: (Optional) Displays information only about LSAs based on inter-area prefix.

- **inter-area router**: (Optional) Displays information only about LSAs based on inter-area router LSAs.

- **link**: (Optional) Displays information about link LSAs. When it follows the **unknown** keyword, the **link** keyword filters link-scope LSAs.

- **link-state-id**: (Optional) Specifies an integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.

- **network**: (Optional) Displays information about network LSAs.

- **nssa-external**: (Optional) Displays information only about the not so stubby area (NSSA) external LSAs.

- **prefix ipv6-prefix**: (Optional) Displays the link-local IPv6 address of the neighbor. The IPv6 prefix must be in the form documented in RFC 2373, in which the address is specified in hexadecimal using 16-bit values between colons.
**process_id**
(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

**ref-lsa**
(Optional) Further filters the prefix LSA type.

**router**
(Optional) Displays information about router LSAs.

**self-originate**
(Optional) Displays only self-originated LSAs from the local router.

---

**Command History**

**Release** | **Modification**
---|---
6.1 | This command was introduced.

---

**Usage Guidelines**

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

---

**Examples**

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

```
> show ipv6 ospf database

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

Router Link States (Area 0)

<table>
<thead>
<tr>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Fragment ID</th>
<th>Link count</th>
<th>Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.4.4</td>
<td>239</td>
<td>0x80000003</td>
<td>0</td>
<td>1</td>
<td>B</td>
</tr>
<tr>
<td>172.16.6.6</td>
<td>239</td>
<td>0x80000003</td>
<td>0</td>
<td>1</td>
<td>B</td>
</tr>
</tbody>
</table>

Inter Area Prefix Link States (Area 0)

<table>
<thead>
<tr>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.4.4</td>
<td>249</td>
<td>0x80000001</td>
<td>FEC0:3344::/32</td>
</tr>
<tr>
<td>172.16.4.4</td>
<td>219</td>
<td>0x80000001</td>
<td>FEC0:3366::/32</td>
</tr>
<tr>
<td>172.16.6.6</td>
<td>247</td>
<td>0x80000001</td>
<td>FEC0:3366::/32</td>
</tr>
<tr>
<td>172.16.6.6</td>
<td>193</td>
<td>0x80000001</td>
<td>FEC0:3344::/32</td>
</tr>
<tr>
<td>172.16.6.6</td>
<td>82</td>
<td>0x80000001</td>
<td>FEC0::/32</td>
</tr>
</tbody>
</table>

Inter Area Router Link States (Area 0)

<table>
<thead>
<tr>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Link ID</th>
<th>Dest RtrID</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.4.4</td>
<td>219</td>
<td>0x80000001</td>
<td>50529027</td>
<td>172.16.3.3</td>
</tr>
<tr>
<td>172.16.6.6</td>
<td>193</td>
<td>0x80000001</td>
<td>50529027</td>
<td>172.16.3.3</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Link ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.4.4</td>
<td>242</td>
<td>0x80000002</td>
<td>14</td>
<td>PO4/0</td>
</tr>
<tr>
<td>172.16.6.6</td>
<td>252</td>
<td>0x80000002</td>
<td>14</td>
<td>PO4/0</td>
</tr>
</tbody>
</table>

Intra Area Prefix Link States (Area 0)

<table>
<thead>
<tr>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Link ID</th>
<th>Ref-lstype</th>
<th>Ref-LSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.4.4</td>
<td>242</td>
<td>0x80000002</td>
<td>0</td>
<td>0x2001</td>
<td>0</td>
</tr>
<tr>
<td>172.16.6.6</td>
<td>252</td>
<td>0x80000002</td>
<td>0</td>
<td>0x2001</td>
<td>0</td>
</tr>
</tbody>
</table>
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 ospf</td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
<tr>
<td>show ipv6 ospf border-routers</td>
<td>Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
</tbody>
</table>
**show ipv6 ospf events**

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show ipv6 ospf events

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

  1 Jul 9 18:49:34.071: Timer Exp: ospfv3_if_ack_delayed 0xda05fad8
  2 Jul 9 18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2, Seq# 80000008, Age 1, Area 10
  3 Jul 9 18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004, Age 0, Area 10
  4 Jul 9 18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005, Age 0, Area 10
  5 Jul 9 18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
  6 Jul 9 18:41:18.902: Starting External processing in area 10
  7 Jul 9 18:41:18.902: Starting External processing
  8 Jul 9 18:41:18.902: Starting Inter-Area SPF in area 10
  9 Jul 9 18:41:18.902: Generic: post_spf_intra 0x0
 10 Jul 9 18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
```
11 Jul 9 18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
12 Jul 9 18:41:18.902: Starting Intra-Area SPF in Area 10
13 Jul 9 18:41:18.903: Starting SPF, wait-interval 5000ms
14 Jul 9 18:41:16.403: Timer Exp: ospfv3_if_ack_delayed 0xda05fad8
15 Jul 9 18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0,
Adv-Rtr 50.100.168.192
16 Jul 9 18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,
Seq# 80000003, Age 1, Area 10

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 ospf</td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
<tr>
<td>show ipv6 ospf border-routers</td>
<td>Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
</tbody>
</table>
show ipv6 ospf flood-list

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display OSPFv3 packet pacing information.

**Examples**

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

```
> show ipv6 ospf flood-list
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
Interface POS4/0, Queue length 1
Link state retransmission due in 14 msec

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

Interface FastEthernet0/0, Queue length 0
Interface ATM3/0, Queue length 0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 ospf</code></td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
<tr>
<td><code>show ipv6 ospf border-routers</code></td>
<td>Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
</tbody>
</table>
show ipv6 ospf graceful-restart

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 ospf</td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
</tbody>
</table>
show ipv6 ospf interface

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 ospf</td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
<tr>
<td>show ipv6 ospf</td>
<td>Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
</tbody>
</table>
show ipv6 ospf request-list

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

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

### Syntax Description

- **area_id**  
  (Optional) Displays information about a specified area only.

- **interface**  
  (Optional) Specifies the list of all LSAs requested by the router from this interface.

- **interface-neighbor**  
  (Optional) Specifies the list of all LSAs requested by the router on this interface from this neighbor.

- **neighbor**  
  (Optional) Specifies the list of all LSAs requested by the router from this neighbor.

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

```
> show ipv6 ospf request-list

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

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

<table>
<thead>
<tr>
<th>Type</th>
<th>LS ID</th>
<th>ADV RTR</th>
<th>Seq NO</th>
<th>Age</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0.0.0</td>
<td>192.168.255.3</td>
<td>0x800000C2</td>
<td>1</td>
<td>0x0014C5</td>
</tr>
<tr>
<td>1</td>
<td>0.0.0.0</td>
<td>192.168.255.2</td>
<td>0x800000C8</td>
<td>0</td>
<td>0x000BCA</td>
</tr>
<tr>
<td>1</td>
<td>0.0.0.0</td>
<td>192.168.255.1</td>
<td>0x800000C5</td>
<td>1</td>
<td>0x008CD1</td>
</tr>
<tr>
<td>2</td>
<td>0.0.0.3</td>
<td>192.168.255.3</td>
<td>0x800000A9</td>
<td>774</td>
<td>0x0058C0</td>
</tr>
<tr>
<td>2</td>
<td>0.0.0.2</td>
<td>192.168.255.3</td>
<td>0x800000B7</td>
<td>1</td>
<td>0x003A63</td>
</tr>
</tbody>
</table>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ipv6 ospf</strong></td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
<tr>
<td><strong>show ipv6 ospf</strong></td>
<td>Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
</tbody>
</table>
**show ipv6 ospf retransmission-list**

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>area_id</strong></td>
</tr>
<tr>
<td><strong>interface</strong></td>
</tr>
<tr>
<td><strong>interface-neighbor</strong></td>
</tr>
<tr>
<td><strong>neighbor</strong></td>
</tr>
<tr>
<td><strong>process_id</strong></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show ipv6 ospf retransmission-list

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

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 ospf</code></td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
<tr>
<td><code>show ipv6 ospf border-routers</code></td>
<td>Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
</tbody>
</table>
show ipv6 ospf statistic

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

SPF 2 executed 04:35:50 ago, SPF type Full
SPF calculation time (in msec):
  SPT  Prefix D-Int Sum D-Sum Ext D-Ext Total
  0     0     0     0     0     0     0     0
RIB manipulation time (in msec):
  RIB Update  RIB Delete
  0     0
LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
Change record R N L
LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R) 50.100.168.192/2(N)
```
show ipv6 ospf summary-prefix

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

`show ipv6 ospf [process_id] summary-prefix`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process_id</td>
<td>(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 ospf</td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
<tr>
<td>show ipv6 ospf border-routers</td>
<td>Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
</tbody>
</table>
show ipv6 ospf timers

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lsa-group</td>
<td>(Optional) Specifies OSPFv3 LSA group information.</td>
</tr>
<tr>
<td>process_id</td>
<td>(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.</td>
</tr>
<tr>
<td>rate-limit</td>
<td>(Optional) Specifies OSPFv3 LSA rate limit information.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show ipv6 ospf timers lsa-group

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

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

Failure Head 0, Last 0 LSA group failure logged

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

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

Failure Head 0, Last 0 LSA group failure logged
```
show ipv6 ospf traffic

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface_name</code></td>
<td>(Optional) Specifies the name of the interface. Use this option to segregate traffic to a specific interface.</td>
</tr>
<tr>
<td><code>process_id</code></td>
<td>(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
show ipv6 ospf 10 traffic inside

Interface inside

Last clearing of interface traffic counters never

OSPFv3 packets received/sent

<table>
<thead>
<tr>
<th>Type</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Invalid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RX Hello</td>
<td>1232</td>
<td>53132</td>
</tr>
<tr>
<td>RX DB des</td>
<td>27</td>
<td>896</td>
</tr>
<tr>
<td>RX LS req</td>
<td>3</td>
<td>216</td>
</tr>
<tr>
<td>RX LS upd</td>
<td>28</td>
<td>2436</td>
</tr>
<tr>
<td>RX LS ack</td>
<td>14</td>
<td>1064</td>
</tr>
<tr>
<td>RX Total</td>
<td>1304</td>
<td>57744</td>
</tr>
<tr>
<td>TX Failed</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TX Hello</td>
<td>753</td>
<td>32072</td>
</tr>
<tr>
<td>TX DB des</td>
<td>27</td>
<td>1056</td>
</tr>
<tr>
<td>TX LS req</td>
<td>2</td>
<td>92</td>
</tr>
<tr>
<td>TX LS upd</td>
<td>9</td>
<td>1128</td>
</tr>
<tr>
<td>TX LS ack</td>
<td>15</td>
<td>900</td>
</tr>
<tr>
<td>TX Total</td>
<td>806</td>
<td>35248</td>
</tr>
</tbody>
</table>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 ospf</code></td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
<tr>
<td><code>show ipv6 ospf border-routers</code></td>
<td>Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
</tbody>
</table>
**show ipv6 ospf virtual-links**

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

show ipv6 ospf virtual-links

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show ipv6 ospf virtual-links

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 ospf</td>
<td>Shows all IPv6 settings in the OSPFv3 routing process.</td>
</tr>
<tr>
<td>show ipv6 ospf border-routers</td>
<td>Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
</tbody>
</table>
show ipv6 prefix-list

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

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

### Syntax Description

- **detail**
  - Show details about prefix lists.

- **summary**
  - Show a summary of prefix lists.

- **prefix_list_name**
  - Name of a prefix list.

- **seq sequence_number**
  - (Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix list.

- **network/length [ longer | first-match ]**
  - (Optional) Displays all entries in the specified prefix list that use this network address and prefix length (in bits).

  You can optionally include one of the following keywords:

  - **longer**
    - displays all entries of the specified prefix list that match or are more specific than the given network/length.

  - **first-match**
    - displays the first entry of the specified prefix list that matches the given network/length.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

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

The following is an example of summarized output.

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

The following is an example of detailed output.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 prefix-list</td>
<td>Reset the hit count on an IPv6 prefix list.</td>
</tr>
<tr>
<td>show bgp prefix-list</td>
<td>Displays information about a prefix list or prefix list entries in the context of Border Gateway Protocol.</td>
</tr>
<tr>
<td>show prefix-list</td>
<td>Displays information about IPv4 prefix lists.</td>
</tr>
</tbody>
</table>

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

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

```
show ipv6 route [management-only] [failover] [cluster] [interface name] [ospf] [summary]
```

**Syntax Description**

- `management-only` (Optional) Displays routes in the IPv6 management routing table.
- `cluster` (Optional) Displays the IPv6 routing table sequence number, IPv6 reconvergence timer status, and IPv6 routing entries sequence number in a cluster.
- `failover` (Optional) Displays the IPv6 routing table sequence number, IPv6 reconvergence timer status, and IPv6 routing entries sequence number.
- `interface name` (Optional) Displays IPv6 interface-specific routes.
- `ospf` (Optional) Displays OSPFv3 routes.
- `summary` (Optional) Displays IPv6 route summaries.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 Level 1—Integrated IS-IS Level 1 derived
  - I2—ISIS Level 2—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:

```plaintext
> 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 ::, outside
S    ::/0 [0/0]
    via fec0::65:0:0:a0a:6575, vlan101
```

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

```plaintext
> show ipv6 route failover

IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired
O    2009::1/128 [110/10]
    via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
    via fe80::217:94ff:fe85:4401, inside seq 0
S    4001::1/128 [0/0]
    via 4001::2, inside seq 0
C    7001::1/128 [0/0]
    via ::, outside seq 0
L   fe80::/10 [0/0]
    via ::, inside seq 0
    via ::, outside seq 0
L   ff00::/8 [0/0]
    via ::, inside seq 0
    via ::, outside seq 0
```

The following is sample output from the **show ipv6 route cluster** command on the master unit:
show ipv6 route cluster

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

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

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

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

> show ipv6 route cluster

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

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show route</td>
<td>Displays the IPv4 routing table.</td>
</tr>
</tbody>
</table>
show ipv6 routers

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

```
show ipv6 routers [if_name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>if_name</code></td>
<td>(Optional) The internal or external interface name that you want to display</td>
</tr>
<tr>
<td></td>
<td>information about.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 route</td>
<td>Adds a static entry to the IPv6 routing table.</td>
</tr>
</tbody>
</table>
show ipv6 traffic

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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:

```plaintext
> 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
  unreachable: 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
  unreachable: 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 traffic</td>
<td>Clears IPv6 traffic counters.</td>
</tr>
</tbody>
</table>
show isakmp sa

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

```
show isakmp sa [detail]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Displays detailed output about the SA database.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays detailed information about the SA database:

```
> show isakmp sa detail
IKE Peer  Type  Dir  Rky  State  Encrypt  Hash  Auth  Lifetime
1 209.165.200.225 User  Resp  No  AM_Active  3des  SHA  preshrd 86400
IKE Peer  Type  Dir  Rky  State  Encrypt  Hash  Auth  Lifetime
2 209.165.200.226 User  Resp  No  AM_ACTIVE  3des  SHA  preshrd 86400
IKE Peer  Type  Dir  Rky  State  Encrypt  Hash  Auth  Lifetime
3 209.165.200.227 User  Resp  No  AM_ACTIVE  3des  SHA  preshrd 86400
IKE Peer  Type  Dir  Rky  State  Encrypt  Hash  Auth  Lifetime
4 209.165.200.228 User  Resp  No  AM_ACTIVE  3des  SHA  preshrd 86400
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isakmp sa</td>
<td>Clears the IKE runtime SA database.</td>
</tr>
<tr>
<td>show running-config isakmp</td>
<td>Displays all the active ISAKMP configuration.</td>
</tr>
</tbody>
</table>
show isakmp stats

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

- Active/Standby Tunnels—`cikePhase1GWActiveTunnels`
- Previous Tunnels—`cikePhase1GWPreviousTunnels`
- In Octets—`cikePhase1GWInOctets`
- In Packets—`cikePhase1GWInPkts`
- In Drop Packets—`cikePhase1GWInDropPkts`
- In Notifys—`cikePhase1GWInNotifys`
- In P2 Exchanges—`cikePhase1GWInP2Exchs`
- In P2 Exchange Invalids—`cikePhase1GWInP2ExchgInvalids`
- In P2 Exchange Rejects—`cikePhase1GWInP2ExchgRejects`
- In P2 Sa Delete Requests—`cikePhase1GWInP2SaDelRequests`
- Out Octets—`cikePhase1GWOutOctets`
- Out Packets—`cikePhase1GWOutPkts`
- Out Drop Packets—`cikePhase1GWOutDropPkts`
- Out Notifys—`cikePhase1GWOutNotifys`
- Out P2 Exchanges—`cikePhase1GWOutP2Exchs`
- Out P2 Exchange Invalids—`cikePhase1GWOutP2ExchgInvalids`
- Out P2 Exchange Rejects—`cikePhase1GWOutP2ExchgRejects`
- Out P2 Sa Delete Requests—`cikePhase1GWOutP2SaDelRequests`
- Initiator Tunnels—`cikePhase1GWinTunnels`
- Initiator Fails—`cikePhase1GWinTunnelFails`
- Responder Fails—`cikePhase1GWRespTunnelFails`
- System Capacity Fails—`cikePhase1GW SysCapFails`
- Auth Fails—`cikePhase1GWAuthFails`
Examples

The following example displays ISAKMP statistics:

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

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isakmp sa</td>
<td>Clears the IKE runtime SA database.</td>
</tr>
<tr>
<td>show running-config isakmp</td>
<td>Displays all the active ISAKMP configuration.</td>
</tr>
</tbody>
</table>
show isis database

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>(Optional) Displays the IS-IS link-state database for Level 1.</td>
</tr>
<tr>
<td>level-2</td>
<td>(Optional) Displays the IS-IS link-state database for Level 2.</td>
</tr>
<tr>
<td>ip</td>
<td>(Optional) Shows the IS-IS link-state database for the IPv4 address-family</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) Shows the IS-IS link-state database for the IPv6 address-family</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays the contents of each link-state packet (LSP).</td>
</tr>
<tr>
<td>verbose</td>
<td>(Optional) Displays additional information about the Intermediate IS-IS database.</td>
</tr>
<tr>
<td>topology base</td>
<td>(Optional) Shows the MTR topology.</td>
</tr>
<tr>
<td>unicast</td>
<td>(Optional) Shows unicast address families.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The following table explains the output for this command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSPID</td>
<td>The Link-state packet (LSP) identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is nonzero, the LSP describes links from the system. When it is zero, the LSP is a so-called nonpseudonode LSP. This mechanism is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP will describe the state of the originating router. For each LAN, the designated router for that LAN will create and flood a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP will be divided into multiple LSP fragments. Each fragment will have a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.</td>
</tr>
<tr>
<td>LSP Seq Num</td>
<td>Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LSP Checksum</td>
<td>Checksum of the entire LSP packet.</td>
</tr>
<tr>
<td>LSP Holdtime</td>
<td>Amount of time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP will stay in the LSDB before being completely removed.</td>
</tr>
<tr>
<td>ATT</td>
<td>The Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers will use the Attach bit to find the closest Level 2 router. They will point a default route to the closest Level 2 router.</td>
</tr>
<tr>
<td>P</td>
<td>The P bit. Detects if the intermediate systems is area partition repair-capable. Cisco and other vendors do not support area partition repair.</td>
</tr>
<tr>
<td>OL</td>
<td>The Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers will not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router will be sent to this router.</td>
</tr>
<tr>
<td>Area Address</td>
<td>Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.</td>
</tr>
<tr>
<td>NLPID</td>
<td>Network Layer Protocol identifier.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname of the node.</td>
</tr>
<tr>
<td>Router ID</td>
<td>Traffic engineering router identifier for the node.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IPv4 address for the interface.</td>
</tr>
<tr>
<td>Metric</td>
<td>IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system (ES), or a Connectionless Network Service [CLNS] prefix).</td>
</tr>
<tr>
<td>Affinity</td>
<td>Link attribute flags that are being flooded.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical BW</strong></td>
<td>Link bandwidth capacity (in bits per second).</td>
</tr>
<tr>
<td><em>(Verbose output only.)</em></td>
<td><strong>Reservable BW</strong> Amount of reservable bandwidth on this link.</td>
</tr>
<tr>
<td><em>(Verbose output only.)</em></td>
<td><strong>BW Unreserved</strong> Amount of bandwidth that is available for reservation.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows the IS-IS database.

> `show isis database`

**IS-IS Level-1 Link State Database:**

<table>
<thead>
<tr>
<th>LSPID</th>
<th>LSP Seq Num</th>
<th>LSP Checksum</th>
<th>LSP Holdtime</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1.00-00</td>
<td>0xea19d300</td>
<td>0x3d0d</td>
<td>674</td>
<td>0/0/0</td>
</tr>
<tr>
<td>routerA.00-00</td>
<td>0x1b541556</td>
<td>0xa349</td>
<td>928</td>
<td>0/0/0</td>
</tr>
<tr>
<td>c3.00-00</td>
<td>0x9257c979</td>
<td>0x9952</td>
<td>759</td>
<td>0/0/0</td>
</tr>
<tr>
<td>c2.00-00</td>
<td>*0xef11e977</td>
<td>0x3188</td>
<td>489</td>
<td>0/0/0</td>
</tr>
<tr>
<td>c2.01-00</td>
<td>*0xa8333f03</td>
<td>0xd6ea</td>
<td>829</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

**IS-IS Level-2 Link State Database:**

<table>
<thead>
<tr>
<th>LSPID</th>
<th>LSP Seq Num</th>
<th>LSP Checksum</th>
<th>LSP Holdtime</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1.00-00</td>
<td>0xe63871f24</td>
<td>0xaba2</td>
<td>526</td>
<td>0/0/0</td>
</tr>
<tr>
<td>routerA.00-00</td>
<td>0x0d540b55</td>
<td>0x81d7</td>
<td>472</td>
<td>0/0/0</td>
</tr>
<tr>
<td>routerA.00-01</td>
<td>*0xffffff01</td>
<td>0xe20b</td>
<td>677</td>
<td>0/0/0</td>
</tr>
<tr>
<td>c3.00-00</td>
<td>0x002e5434</td>
<td>0xb20a</td>
<td>487</td>
<td>0/0/0</td>
</tr>
<tr>
<td>c2.00-00</td>
<td>*0x74fd1227</td>
<td>0xbb0f</td>
<td>742</td>
<td>0/0/0</td>
</tr>
<tr>
<td>c2.01-00</td>
<td>*0x7ee72c1a</td>
<td>0xb506</td>
<td>968</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

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

> `show isis database detail`

**IS-IS Level-1 Link State Database:**

<table>
<thead>
<tr>
<th>LSPID</th>
<th>LSP Seq Num</th>
<th>LSP Checksum</th>
<th>LSP Holdtime</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1.00-00</td>
<td>0xea19d301</td>
<td>0x3b0e</td>
<td>1189</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>
| Area Address: 49.0001  
NLPID: 0xcc  
Hostname: c1  
IP Address: 10.22.22.1  
Metric: 10 IP 10.22.22.0 255.255.255.0  
Metric: 10 IS c2.01  
routerA.00-00 | 0x1b541556  | 0xa349       | 642          | 0/0/0    |
| Area Address: 49.0001  
NLPID: 0xcc  
Hostname: routerA  
IP Address: 10.22.22.5 |
The following example shows detailed output for a Level 2 LSP only. The area address 39.0001 is the address of the area in which the router resides.

```bash
> show isis database 12 detail
```

**IS-IS Level-2 Link State Database:**

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

The following example shows verbose output.

```bash
> show isis database verbose
```

**IS-IS Level-1 Link State Database:**

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isis</td>
<td>Clears IS-IS data structures.</td>
</tr>
<tr>
<td>show clns</td>
<td>Shows CLNS-specific information.</td>
</tr>
<tr>
<td>show route isis</td>
<td>Shows IS-IS routes.</td>
</tr>
</tbody>
</table>
show isis hostname

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

### Examples

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

```
> show isis hostname

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isis</td>
<td>Clears IS-IS data structures.</td>
</tr>
<tr>
<td>show clns</td>
<td>Shows CLNS-specific information.</td>
</tr>
<tr>
<td>show route isis</td>
<td>Shows IS-IS routes.</td>
</tr>
</tbody>
</table>
show isis lsp-log

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

```plaintext
> show isis lsp-log

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

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isis</td>
<td>Clears IS-IS data structures.</td>
</tr>
<tr>
<td>show clns</td>
<td>Shows CLNS-specific information.</td>
</tr>
<tr>
<td>show route isis</td>
<td>Shows IS-IS routes.</td>
</tr>
</tbody>
</table>
show isis neighbors

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

```
show isis neighbors [ detail ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Displays more detailed information for IS-IS neighbors.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The following table explains the IS-IS neighbor information.

**Table 44: IS-IS Neighbor Information**

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

```plaintext
> show isis neighbors

+--------+-------+--------+---------+---------+---------+
<table>
<thead>
<tr>
<th>System Id</th>
<th>Type</th>
<th>Interface</th>
<th>IP Address</th>
<th>State</th>
<th>Holdtime</th>
<th>Circuit Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>routerA</td>
<td>L1</td>
<td>subint</td>
<td>10.22.22.5</td>
<td>UP</td>
<td>21</td>
<td>c2.01</td>
</tr>
<tr>
<td>routerA</td>
<td>L2</td>
<td>subint</td>
<td>10.22.22.5</td>
<td>UP</td>
<td>22</td>
<td>c2.01</td>
</tr>
<tr>
<td>c2</td>
<td>L1</td>
<td>subint</td>
<td>10.22.22.3</td>
<td>UP</td>
<td>9</td>
<td>c2.01</td>
</tr>
<tr>
<td>c2</td>
<td>L2</td>
<td>subint</td>
<td>10.22.22.3</td>
<td>UP</td>
<td>9</td>
<td>c2.01</td>
</tr>
</tbody>
</table>
```

The following example shows detailed IS-IS neighbor information.

```plaintext
> show isis neighbors detail

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isis</td>
<td>Clears IS-IS data structures.</td>
</tr>
<tr>
<td>show clns</td>
<td>Shows CLNS-specific information.</td>
</tr>
<tr>
<td>show route isis</td>
<td>Shows IS-IS routes.</td>
</tr>
</tbody>
</table>
show isis rib

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

```
> show isis rib

IPv4 local RIB for IS-IS process
IPV4 unicast topology base (TID 0, TGPOID 0x2) - - - - - - - - - - - - - -
10.10.0.0 255.255.0.0
 [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]

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

10.3.2.0 255.255.255.0
 [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```
The following example shows all routes under the major network 10.0.0.0 with the IP address 10.3.2.0 that are stored within the IS-IS local RIB.

> **show isis rib 10.3.2.0**

IPv4 local RIB for IS-IS process

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

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

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

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

> **show isis rib 10.3.2.0 255.255.255.0**

IPv4 local RIB for IS-IS process

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isis</td>
<td>Clears IS-IS data structures.</td>
</tr>
<tr>
<td>show clns</td>
<td>Shows CLNS-specific information.</td>
</tr>
<tr>
<td>show route isis</td>
<td>Shows IS-IS routes.</td>
</tr>
</tbody>
</table>
**show isis spf-log**

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

**Examples**

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

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isis</td>
<td>Clears IS-IS data structures.</td>
</tr>
<tr>
<td>show clns</td>
<td>Shows CLNS-specific information.</td>
</tr>
<tr>
<td>show route isis</td>
<td>Shows IS-IS routes.</td>
</tr>
</tbody>
</table>
show isis topology

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

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

**Syntax Description**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

**Examples**

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

```
> show isis topology
IS-IS TID 0 paths to level-1 routers
System Id   Metric   Next-Hop     Interface   SNPA
 Cisco1      --       --           --          --
routerA      10       routerA     subint     0025.8407.f2b0
c3           10       --           --          --
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isis</td>
<td>Clears IS-IS data structures.</td>
</tr>
<tr>
<td>show clns</td>
<td>Shows CLNS-specific information.</td>
</tr>
<tr>
<td>show route isis</td>
<td>Shows IS-IS routes.</td>
</tr>
</tbody>
</table>
show j - show o

- show jumbo-frame reservation, on page 685
- show kernel, on page 686
- show lacp, on page 690
- show lacp cluster, on page 692
- show lisp eid, on page 693
- show local-host, on page 694
- show log-events-to-ramdisk, on page 698
- show logging, on page 699
- show mac-address-table, on page 703
- show mac-learn, on page 704
- show managers, on page 705
- show memory, on page 707
- show memory delayed-free-poisoner, on page 712
- show memory logging, on page 713
- show memory profile, on page 715
- show memory tracking, on page 717
- show memory webvpn, on page 719
- show mfib, on page 721
- show mgcp, on page 724
- show mode, on page 726
- show model, on page 727
- show module, on page 728
- show monitor-interface, on page 731
- show mrib client, on page 732
- show mrib route, on page 734
- show mroute, on page 736
- show nameif, on page 739
- show nat, on page 741
- show nat divert-table, on page 743
- show nat pool, on page 745
- show nat proxy-arp, on page 747
- show network, on page 748
- show network-dhcp-server, on page 749
• show network-static-routes, on page 750
• show ntp, on page 751
• show object-group, on page 753
• show ospf, on page 754
• show ospf border-routers, on page 756
• show ospf database, on page 757
• show ospf events, on page 760
• show ospf flood-list, on page 761
• show ospf interface, on page 762
• show ospf neighbor, on page 763
• show ospf nsf, on page 764
• show ospf request-list, on page 765
• show ospf retransmission-list, on page 766
• show ospf rib, on page 767
• show ospf statistics, on page 768
• show ospf summary-address, on page 769
• show ospf traffic, on page 770
• show ospf virtual-links, on page 771
**show jumbo-frame reservation**

To view whether jumbo frames are enabled for all interfaces, use the `show jumbo-frame reservation` command.

---

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Jumbo frame reservation is enabled whenever you increase the MTU for any interface over 1500. It is automatically disabled when you return all MTUs to 1500 or lower.

**Examples**

The following is sample output from the `show jumbo-frame reservation` command when jumbo frame support is enabled:

```plaintext
> show jumbo-frame-reservation
Jumbo Frame Support is currently enabled
```
show kernel

To display information that the Linux brctl utility provides that you can use for debugging, use the **show kernel** command.

```
show kernel [process | bridge [mac-address bridge_name] | cgroup-controller [cpu | cpuset | memory] [detail] | ifconfig | module]
```

### Syntax Description

**bridge [mac-address bridge_name]**

Displays the Linux tap bridges, their member ports, and the MAC addresses that have been learned at each port (including remote MAC addresses) that you can use for debugging. You can use the **mac-address** keyword to view MAC address details about a specific bridge. Use the command without the keyword to see the available bridge names, such as br0.

**cgroup-controller [cpu | cpuset | memory] [detail]**

Displays the cgroup-controller statistics. The **cpu**, **cpuset** and **memory** keywords allow you to filter the cgroup-controller statistics as per your requirements. Use the **detail** keyword to see extra information.

**ifconfig**

Displays the tap and bridge interface statistics.

**module**

Displays the modules that are installed and running.

**process**

Displays the current status of the active kernel processes running on the device.

### Command History

**Release** | **Modification**
---|---
6.1 | This command was introduced.

### Usage Guidelines

This command displays statistics for the various processes running on the kernel.

### Examples

The following example displays output from the **show kernel process** command:

```
> show kernel process

<table>
<thead>
<tr>
<th>PID</th>
<th>PPID</th>
<th>PRI</th>
<th>NI</th>
<th>VSIZE</th>
<th>RSS</th>
<th>WCHAN</th>
<th>STAT</th>
<th>RUNTIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>16</td>
<td>0</td>
<td>991232</td>
<td>268</td>
<td>3725684979</td>
<td>S</td>
<td>78</td>
<td>init</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>34</td>
<td>19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>10</td>
<td>-5</td>
<td>0</td>
<td>0</td>
<td>3725736671</td>
<td>S</td>
<td>0</td>
<td>events/0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>10</td>
<td>-5</td>
<td>0</td>
<td>0</td>
<td>3725736671</td>
<td>S</td>
<td>0</td>
<td>helper</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>20</td>
<td>-5</td>
<td>0</td>
<td>0</td>
<td>3725736671</td>
<td>S</td>
<td>0</td>
<td>kthread</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>10</td>
<td>-5</td>
<td>0</td>
<td>0</td>
<td>3725736671</td>
<td>S</td>
<td>0</td>
<td>kblockd/0</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>20</td>
<td>-5</td>
<td>0</td>
<td>0</td>
<td>3726794334</td>
<td>S</td>
<td>0</td>
<td>kseriod</td>
</tr>
<tr>
<td>66</td>
<td>5</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3725811768</td>
<td>S</td>
<td>0</td>
<td>pdflush</td>
</tr>
<tr>
<td>67</td>
<td>5</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3725811768</td>
<td>S</td>
<td>0</td>
<td>pdflush</td>
</tr>
<tr>
<td>68</td>
<td>1</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3725824451</td>
<td>S</td>
<td>2</td>
<td>kswapd0</td>
</tr>
<tr>
<td>69</td>
<td>5</td>
<td>20</td>
<td>-5</td>
<td>0</td>
<td>0</td>
<td>3725736671</td>
<td>S</td>
<td>0</td>
<td>aio/0</td>
</tr>
<tr>
<td>171</td>
<td>1</td>
<td>16</td>
<td>0</td>
<td>991232</td>
<td>80</td>
<td>3725684979</td>
<td>S</td>
<td>0</td>
<td>init</td>
</tr>
<tr>
<td>172</td>
<td>171</td>
<td>19</td>
<td>0</td>
<td>983040</td>
<td>268</td>
<td>3725684979</td>
<td>S</td>
<td>0</td>
<td>rcS</td>
</tr>
<tr>
<td>201</td>
<td>172</td>
<td>21</td>
<td>0</td>
<td>1351680</td>
<td>344</td>
<td>3725712932</td>
<td>S</td>
<td>0</td>
<td>lina_monitor</td>
</tr>
<tr>
<td>202</td>
<td>201</td>
<td>16</td>
<td>0</td>
<td>1017602048</td>
<td>899932</td>
<td>3725716348</td>
<td>S</td>
<td>212</td>
<td>lina</td>
</tr>
<tr>
<td>203</td>
<td>202</td>
<td>16</td>
<td>0</td>
<td>1017602048</td>
<td>899932</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>lina</td>
</tr>
</tbody>
</table>
```
The following table explains each field.

**Table 45: show kernel process Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>The process ID.</td>
</tr>
<tr>
<td>PPID</td>
<td>The parent process ID.</td>
</tr>
<tr>
<td>PRI</td>
<td>The priority of the process.</td>
</tr>
<tr>
<td>NI</td>
<td>The nice value, which is used in priority computation. The values range from 19 (nicest) to -19 (not nice to others).</td>
</tr>
<tr>
<td>VSIZE</td>
<td>The virtual memory size in bytes.</td>
</tr>
<tr>
<td>RSS</td>
<td>The resident set size of the process, in kilobytes.</td>
</tr>
<tr>
<td>WCHAN</td>
<td>The channel in which the process is waiting.</td>
</tr>
</tbody>
</table>
| STAT  | The state of the process:  
- R—Running  
- S—Sleeping in an interruptible wait  
- D—Waiting in an uninterruptible disk sleep  
- Z—zombie  
- T—Traced or stopped (on a signal)  
- P—Paging |
| RUNTIME | The number of jiffies that the process has been scheduled in user mode and kernel mode. The runtime is the sum of utime and stime. |
| COMMAND | The process name. |

The following example displays output from the **show kernel module** command:

```markdown
> show kernel module

<table>
<thead>
<tr>
<th>Module</th>
<th>Size</th>
<th>Used by</th>
<th>Tainted: P</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpp_base</td>
<td>861808</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>kvm_intel</td>
<td>44104</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>kvm</td>
<td>174304</td>
<td>1</td>
<td>kvm_intel</td>
</tr>
<tr>
<td>msrif</td>
<td>4180</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>tcsync</td>
<td>3852</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

The following example displays output for the **show kernel ifconfig** command:
The following example displays output from the **show kernel bridge** command:
show kernel bridge

bridge name  bridge id                  STP enabled  interfaces
br0          8000.00000000040001      no           tap1
br1          8000.84b261b192bd      no           tap2
tap3
          tap4
          tap5

The following example displays output from the `show kernel bridge mac-address` command:

> show kernel bridge mac-address br1

port no  mac addr  is local?  ageing timer
1  00:21:d8:cb:dc:f7  no        12.93
3  00:22:bd:d8:7d:da  no        12.93
2  26:d2:9f:51:a4:90  yes       0.00
1  4e:a4:e0:73:1f:ab  yes       0.00
3  52:04:38:3d:79:c0  yes       0.00

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show module</td>
<td>Shows information about the installed modules in the device.</td>
</tr>
</tbody>
</table>
show lacp

To display EtherChannel LACP information such as traffic statistics, system identifier, and neighbor details, enter this command.

```
show lacp {channel_group_number [counters | internal [detail] | neighbor [detail]] | neighbor [detail] | sys-id}
```

**Syntax Description**

- `channel_group_number`: Specifies the EtherChannel channel group number, between 1 and 48, and only shows information about this channel group.
- `counters`: Shows counters for the number of LACPDUs and markers sent and received.
- `detail`: Shows additional detail for the item.
- `internal`: Shows internal information.
- `neighbor`: Shows neighbor information.
- `sys-id`: Shows the LACP system ID.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show lacp sys-id` command:

```
> show lacp sys-id
32768,001c.c4e5.cfee
```

The following is sample output from the `show lacp counters` command:

```
> show lacp counters

<table>
<thead>
<tr>
<th>Port</th>
<th>LACPDUs</th>
<th>Marker</th>
<th>Marker Response</th>
<th>LACPDUs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sent</td>
<td>Sent</td>
<td>Recv</td>
<td>Sent</td>
</tr>
<tr>
<td></td>
<td>Pkts</td>
<td>Err</td>
<td></td>
<td>Pkts</td>
</tr>
</tbody>
</table>

Channel group: 1
Gi3/1  736  728  0  0  0  0  0  0
Gi3/2  739  730  0  0  0  0  0  0
Gi3/3  739  732  0  0  0  0  0  0
```

The following is sample output from the `show lacp internal` command:

```
> show lacp internal

Flags:  S = Device is requesting Slow LACPDUs
        F = Device is requesting Fast LACPDUs
        A = Device is in Active mode
        P = Device is in Passive mode
```
Channel group 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>LACP port</th>
<th>Admin Priority</th>
<th>Oper Key</th>
<th>Port Number</th>
<th>Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/1</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x302</td>
<td>0x3d</td>
</tr>
<tr>
<td>Gi3/2</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x303</td>
<td>0x3d</td>
</tr>
<tr>
<td>Gi3/3</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x304</td>
<td>0x3d</td>
</tr>
</tbody>
</table>

The following is sample output from the `show lacp neighbor` command:

> show lacp neighbor

Flags:  
- S - Device is requesting Slow LACPDUs  
- F - Device is requesting Fast LACPDUs  
- A - Device is in Active mode  
- P - Device is in Passive mode

Channel group 1 neighbors

<table>
<thead>
<tr>
<th>Partner's information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Flags State</td>
</tr>
<tr>
<td>Gi3/1 SA bndl</td>
</tr>
<tr>
<td>Gi3/2 SA bndl</td>
</tr>
<tr>
<td>Gi3/3 SA bndl</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show port-channel</td>
<td>Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.</td>
</tr>
<tr>
<td>show port-channel load-balance</td>
<td>Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.</td>
</tr>
</tbody>
</table>
show lacp cluster

To show the cLACP system MAC and ID, use the `show lacp cluster` command:

```
show lacp cluster { system-mac | system-id }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system-mac</td>
<td>Shows the system ID and whether it was auto-generated or entered manually.</td>
</tr>
<tr>
<td>system-id</td>
<td>Shows the system ID and priority.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show lacp cluster system-mac` command:

```
> show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

The following is sample output from the `show lacp cluster system-id` command:

```
> show lacp cluster system-id
5 ,a300.010a.010a
```
show lisp eid

To view the EID table, use the **show lisp eid** command.

```
show lisp eid  [site-id  id]
```

**Syntax Description**

| site-id | id       | View only EIDs for a particular site. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The device maintains an EID table that correlates the EID and the site ID.

**Examples**

The following is sample output from the **show lisp eid** command:

```
> show lisp eid
LISP EID       Site ID
10.44.33.105   2
10.44.33.201   2
192.168.11.1   4
192.168.11.2   4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear cluster info flow-mobility counters</td>
<td>Clears the flow mobility counters.</td>
</tr>
<tr>
<td>clear lisp eid</td>
<td>Removes EIDs from the ASA EID table.</td>
</tr>
<tr>
<td>show cluster info flow-mobility counters</td>
<td>Shows flow mobility counters.</td>
</tr>
<tr>
<td>show conn</td>
<td>Shows traffic subject to LISP flow-mobility.</td>
</tr>
<tr>
<td>show service-policy</td>
<td>Shows the service policy.</td>
</tr>
</tbody>
</table>
show local-host

To display the network states of local hosts, use the `show local-host` command.

```
show local-host [hostname | ip_address] [detail] [all] [brief] [connection {sctp | tcp | udp | embryonic}] start[-end] [zone]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) Includes local hosts connecting to and from the device.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays brief information on local hosts.</td>
</tr>
<tr>
<td>connection {sctp</td>
<td>tcp</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays the detailed network states of local host information, including more information about active xlates and network connections.</td>
</tr>
<tr>
<td>hostname</td>
<td>ip_address</td>
</tr>
<tr>
<td>zone</td>
<td>(Optional) Specifies local hosts per zone or inline set.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `show local-host` command lets you display the network states of local hosts. A local-host is created for any host that forwards traffic to, or through, the Firepower Threat Defense device.

This command lets you show the translation and connection slots for the local hosts. Translation information includes any PAT port blocks allocated to the host.

This command also displays the connection limit values. If a connection limit is not set, the value displays as 0 and the limit is not applied.

In the event of a SYN attack (with TCP intercept configured), the `show local-host` command output includes the number of intercepted connections in the usage count. This field typically displays only full open connections.

In the `show local-host` command output, the **TCP embryonic count to host counter** is used when a maximum embryonic limit (TCP intercept watermark) is configured for a host using a static connection. This counter shows the total embryonic connections to the host from other hosts. If this total exceeds the maximum configured limit, TCP intercept is applied to new connections to the host.

### Examples

The following is sample output from the `show local-host` command:

```
> show local-host
```
Interface mgmt: 2 active, 2 maximum active, 0 denied
local host: <10.24.250.191>,
  SCTP flow count/limit = 0/unlimited
  TCP flow count/limit = 1/unlimited
  TCP embryonic count to host = 0
  TCP intercept watermark = unlimited
  UDP flow count/limit = 0/unlimited
local host: <10.44.64.65>,
  SCTP flow count/limit = 0/unlimited
  TCP flow count/limit = 1/unlimited
  TCP embryonic count to host = 1
  TCP intercept watermark = unlimited
  UDP flow count/limit = 5/unlimited
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
Interface any: 0 active, 0 maximum active, 0 denied

The following examples show the network states of local hosts:

> show local-host all

Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
  SCTP flow count/limit = 0/unlimited
  TCP flow count/limit = 0/unlimited
  TCP embryonic count to host = 0
  TCP intercept watermark = unlimited
  UDP flow count/limit = 0/unlimited
Conn:
  105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
  105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
  SCTP flow count/limit = 0/unlimited
  TCP flow count/limit = 0/unlimited
  TCP embryonic count to host = 0
  TCP intercept watermark = unlimited
  UDP flow count/limit = 0/unlimited
Conn:
  105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
  105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
  SCTP flow count/limit = 0/unlimited
  TCP flow count/limit = 0/unlimited
  TCP embryonic count to host = 0
  TCP intercept watermark = unlimited
  UDP flow count/limit = 0/unlimited
Conn:
  105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
  105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
  SCTP flow count/limit = 0/unlimited
  TCP flow count/limit = 0/unlimited
  TCP embryonic count to host = 0
  TCP intercept watermark = unlimited
  UDP flow count/limit = 0/unlimited
Conn:
  105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
  105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
The following example shows information about a specific host, followed by detailed information for that host.

> **show local-host 10.1.1.91**

Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

> **show local-host 10.1.1.91 detail**

Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active,
1 maximum active, 0 denied

The following example shows all hosts who have at least four UDP connections and have between one to 10 TCP connections at the same time:

> **show local-host connection udp 4 tcp 1-10**

Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
watermark = unlimited UDP flow count/limit = 4/unlimited

Xlate:
Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
maximum active, 0 denied
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>clear local-host</strong></td>
<td>Releases network connections from local hosts displayed by the <code>show local-host</code> command.</td>
</tr>
</tbody>
</table>
show log-events-to-ramdisk

To display the status of logging connection events to RAM disk, use the `show log-events-to-ramdisk` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command shows whether you are logging connection events to RAM disk or to the Solid State Drive (SSD). RAM disk logging is not supported on all hardware models. You configure RAM disk logging with the `configure log-events-to-ramdisk` command.

### Examples

The following example shows that logging to RAM disk is not supported on this hardware model.

```
> show log-events-to-ramdisk
This command is not available on this platform.
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>Enables or disables logging connection events to RAM disk.</td>
</tr>
<tr>
<td>log-events-to-ramdisk</td>
<td></td>
</tr>
</tbody>
</table>
# show logging

To show the logs in the buffer or other logging settings, use the **show logging** command.

```plaintext
show logging [message [syslog_id | all] | asdm | flow-export-syslogs | queue | setting | unified-client [statistics]]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>(Optional) Displays all syslog message IDs, along with whether they are enabled or disabled.</td>
</tr>
<tr>
<td><code>asdm</code></td>
<td>(Optional) This keyword does not work for Firepower Device Manager. It relates to ASDM, which configures ASA Software devices.</td>
</tr>
<tr>
<td><code>flow-export-syslogs</code></td>
<td>(Optional). Display all of the syslog messages whose information is also captured by NetFlow.</td>
</tr>
<tr>
<td>`message [syslog_id</td>
<td>all]`</td>
</tr>
<tr>
<td><code>queue</code></td>
<td>(Optional) Displays the syslog message queue.</td>
</tr>
<tr>
<td><code>setting</code></td>
<td>(Optional) Displays the logging setting, without displaying the logging buffer.</td>
</tr>
<tr>
<td><code>syslog_id</code></td>
<td>(Optional) Specifies a message number to display.</td>
</tr>
<tr>
<td><code>unified-client [statistics]</code></td>
<td>Shows detailed statistics about the status of the syslog client including the loggerD service status, syslog client registration information, loggerD heartbeat details, and syslog client control/data and error statistics,</td>
</tr>
</tbody>
</table>

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.3</td>
<td>The <strong>unified-client [statistics]</strong> keyword was added.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

If you enable logging to the internal buffer, the **show logging** command without any keywords shows the current message buffer and the current settings.

The **show logging queue** command allows you to display the following:

- Number of messages that are in the queue
- Highest number of messages recorded that are in the queue
- Number of messages that are discarded because block memory was not available to process them
- Separate queues for traps and other syslog messages
Zero is an acceptable number for the configured queue size and represents the maximum queue size allowed. The output for the show logging queue command will display the actual queue size if the configured queue size is zero.

The show logging flow-export-syslogs command shows whether the following syslogs are enabled or disabled. When using Netflow, you have the option of disabling these syslogs because they are redundant.

<table>
<thead>
<tr>
<th>Syslog Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>106015</td>
<td>A TCP flow was denied because the first packet was not a SYN packet.</td>
</tr>
<tr>
<td>106023</td>
<td>A flow that is denied by an ingress ACL or an egress ACL that is attached to an interface.</td>
</tr>
<tr>
<td>106100</td>
<td>A flow that is permitted or denied by an ACL.</td>
</tr>
<tr>
<td>302013 and 302014</td>
<td>A TCP connection and deletion.</td>
</tr>
<tr>
<td>302015 and 302016</td>
<td>A UDP connection and deletion.</td>
</tr>
<tr>
<td>302017 and 302018</td>
<td>A GRE connection and deletion.</td>
</tr>
<tr>
<td>302020 and 302021</td>
<td>An ICMP connection and deletion.</td>
</tr>
<tr>
<td>313001</td>
<td>An ICMP packet to the Firepower Threat Defense device was denied.</td>
</tr>
<tr>
<td>313008</td>
<td>An ICMPv6 packet to the Firepower Threat Defense device was denied.</td>
</tr>
<tr>
<td>710003</td>
<td>An attempt to connect to the Firepower Threat Defense was denied.</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the show logging command:

```
> show logging
Syslog logging: enabled
   Facility: 20
   Timestamp logging: enabled
   Standby logging: disabled
   Debug-trace logging: disabled
   Console logging: level informational, 3962 messages logged
   Monitor logging: disabled
   Buffer logging: disabled
   Trap logging: level informational, facility 20, 20549 messages logged
   Logging to inside 10.2.5.3 tcp/50001 connected
   Permit-hostdown state
   History logging: disabled
   Device ID: disabled
   Mail logging: disabled
   ASDM logging: disabled
```
The possible values for Syslog Logging are enabled, disabled, disabled-blocking, and disabled-not-blocking.

The following is sample output from the `show logging` command with a secure syslog server configured:

```
> show logging
Syslog logging: disabled
  Facility:
  Timestamp logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: level debugging, 135 messages logged
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: list show _syslog, facility, 20, 21 messages logged
    Logging to inside 10.0.0.1 tcp/1500 SECURE
  History logging: disabled
  Device ID: disabled
  Mail logging: disabled
  ASDM logging disabled
```

The following is sample output from the `show logging queue` command:

```
> show logging queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

The following is sample output from the `show logging message all` command:

```
> show logging message all
syslog 11111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

The following is sample output from the `show logging unified-client` command:

```
> show logging unified-client
Log client details:
  Name : Lina
  Id : 1331
  Init time : Fri Sep 7 07:20:14 2018
  Status : Registered
```
The following is sample output from the `show logging unified-client statistics` command:

```
> show logging unified-client statistics
Log client details:  
  Name : Lina  
  Id   : 1331  
  Init time : Fri Sep 7 07:20:14 2018  
  Status : Registered  

Loggerd service up/down statistics:  
  Service status : Up  
  Instance-id : 4602  
  Last service down time : Wed Sep 12 05:17:43 2018

Log client register/unregister statistics:  
  Total register messages Tx : 1222  
  Total unregister messages Tx : 0  
  Last register message Tx time : Wed Sep 12 05:40:16 2018  
  Total register-ack messages Rx : 39  
  Last register-ack Rx time : Wed Sep 12 05:40:17 2018  
  Total configuration sent messages Tx : 14  
  Number of configuration pushes : 38

Heartbeat statistics:  
  Last heartbeat Tx time : Wed Sep 12 06:38:33 2018  
  Last Tx seqnum : 10019  
  Total heartbeat Tx : 9981

Loggerd heartbeat statistics:  
  Last heartbeat Rx time : Wed Sep 12 06:38:36 2018  
  Last heartbeat Rx seqnum : 701  
  Total heartbeat Rx : 5977  
  Miss count : 1

Log client data messages details:  
  Syslogs Tx for ngfw-management : 6554  
  Syslogs Rx for data ports : 0  
  Syslogs Tx drops for ngfw-management : 0

Log client Control/Data channel statistics:  
  Total control messages Tx : 11757  
  Total service messages Rx : 98  
  Total notify messages Rx : 6020  
  Total data messages Rx : 0

Log-client error statistics:  
  Register messages Tx : 2373  
  Register-ack messages Rx : 5921  
  Configuration push Tx : 1  
  Heartbeat Tx : 0  
  Control channel Rx : 0  
  Data channel Rx : 0  
  Syslogs Rx for data ports : 0
```
show mac-address-table

To show the MAC address table, use the **show mac-address-table** command.

```
show mac-address-table [interface_name | count | static]
```

### Syntax Description

- **count** (Optional) Lists the total number of dynamic and static entries.
- **interface_name** (Optional) Identifies the interface name for which you want to view MAC address table entries.
- **static** (Optional) Lists only static entries.

### Command Default

If you do not specify an interface, all interface MAC address entries are shown.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was added.</td>
</tr>
<tr>
<td>6.2</td>
<td>We added support in routed firewall mode when using Integrated Routing and Bridging.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the **show mac-address-table** command:

```
> show mac-address-table
interface    mac address    type   Time Left
outside       0009.7cbe.2100  static  -
inside        0010.7cbe.6101  static  -
inside        0009.7cbe.5101  dynamic 10
```

The following is sample output from the **show mac-address-table count** command:

```
> show mac-address-table count
Static       mac-address bridges (curr/max): 0/65535
Dynamic      mac-address bridges (curr/max): 103/65535
```
show mac-learn

To show whether MAC learning is enabled or disabled for each interface, use the **show mac-learn** command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was added.</td>
</tr>
<tr>
<td>6.2</td>
<td>We added support in routed firewall mode when using Integrated Routing and Bridging.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, each interface automatically learns the MAC addresses of entering traffic, and the system adds corresponding entries to the MAC address table. You can disable MAC learning per interface.

**Examples**

The following is sample output from the **show mac-learn** command.

```
> show mac-learn
no mac-learn flood
interface           mac learn
outside             enabled
inside_2            enabled
inside_3            enabled
inside_4            enabled
inside_5            enabled
inside_6            enabled
inside_7            enabled
inside_8            enabled
diagnostic          enabled
inside              enabled
```
show managers

To show the current manager that is managing the device configuration, use the `show managers` command.

```
show managers
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show managers` command to determine which application is defined for managing the device configuration. You can then log into the manager using a web browser.

When you configure a remote manager, Firepower Management Center, for the device using the `configure manager add` command, the output shows the host address and registration status. The registration key and NAT ID are only displayed if registration is pending. If a device is registered to a high availability pair, information about both managing Management Centers is displayed. If a device is configured as a secondary device in a stacked configuration, information about both the managing Management Center and the primary device is displayed.

**Examples**

The following example shows a completed registration to a Firepower Management Center remote manager.

```
> show managers
Type : Manager
Host : 10.83.57.41
Registration : Completed
```

The following example shows that the local manager, Firepower Device Manager, is enabled.

```
> show managers
Managed locally.
```

The following example shows that no manager is currently configured. You must use the `configure manager add` or `configure manager local` to enable one before you can configure the device.

```
> show managers
No managers configured.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure manager add</code></td>
<td>Adds a remote manager, Firepower Management Center.</td>
</tr>
<tr>
<td><code>configure manager delete</code></td>
<td>Deletes the current manager and enters No Manager Mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>configure manager local</td>
<td>Enables the local manager, Firepower Device Manager.</td>
</tr>
</tbody>
</table>
show memory

To display a summary of the maximum physical memory and current free memory available to the operating system, use the show memory command.

```
show memory [api | app-cache | binsize size | caller-address | detail | region | system | top-usage [num]]
```

**Syntax Description**

- **api** (Optional) Displays the malloc stack APIs that are registered in the system. If any of the memory debugging features are turned on (that is, delay-free-poisoner, memory logger, memory tracker, or memory profiler), their APIs appear in the output.

- **app-cache** (Optional) Displays memory usage by application.

- **binsize size** (Optional) Displays summary information about the chunks (memory blocks) allocated for a specific bin size. The bin size is from the “fragment size” column of the show memory detail command output.

- **caller-address** Displays information related to the memory caller-address configuration.

- **detail** (Optional) Displays a detailed view of free and allocated system memory.

- **region** Displays process maps.

- **system** Displays the total memory, the memory in use, and the available memory for the device.

- **top-usage [num]** Displays the top number of allocated fragment sizes from the show memory detail command. You can optionally specify the number of bin sizes to list, from 1-64. The default is 10.

**Command History**

**Release** | **Modification**
--- | ---
6.1 | This command was introduced.
6.2.2 | Output was changed for show memory and show memory detail.

**Usage Guidelines**

The show memory command lets you display a summary of the maximum physical memory and current free memory available to the operating system. Memory is allocated as needed.

You can also display the information from the show memory command using SNMP.

You can use the show memory detail output with the show memory binsize command to debug memory leaks.

The show memory detail command output can be broken down into three sections: Summary, DMA Memory, and HEAP Memory. The summary displays how the total memory is allocated. Memory that is not tied to DMA or reserved is considered the HEAP. The Free Memory value is the unused memory in the HEAP. The Allocated memory in use value is how much of the HEAP has been allocated. The breakdown of HEAP
allocation is displayed later in the output. Reserved memory and DMA Reserved memory are used by different system processes and primarily VPN services.

The Free memory is divided into two parts: Free memory heap and Free memory system. Free memory heap is the amount of free memory in the glibc heap. As the glibc heap grows and shrinks on demand, the amount of free heap memory does not indicate the total memory left in the system. Free memory system represents the amount of free memory available to the ASA.

Reserved memory (DMA) is the amount of memory reserved for the DMA pools. Memory overhead is the glibc overhead and process overhead of various running processes.

Values displayed in the allocated memory statistics total (bytes) column do not reflect real values (MEMPOOL_GLOBAL_SHARED POOL STATS) in the `show memory detail` command output.

**Note**

MEMPOOL_GLOBAL_SHARED does not take all the system memory during bootup, but asks the underlying operating system for memory whenever required. Similarly, it returns memory to the system when a significant amount of memory is freed. As a result, the size of MEMPOOL_GLOBAL_SHARED appears to grow and shrink according to demand. A minimal amount of free memory remains in MEMPOOL_GLOBAL_SHARED to speed up allocation.

The output shows that the block of size 49,152 was allocated then returned to the free pool, and another block of size 131,072 was allocated. In this case, you would think that free memory decreased by 131,072-49,152=81,920 bytes, but it actually decreased by 100,000 bytes (see the Free memory line).

```
> show memory detail
MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated = 1862270976
Number of free chunks = 99
Number of mmapped regions = 0
Mmapped bytes allocated = 0
Max memory footprint = 1862270976
Keepcost = 1762019304
Max contiguous free mem = 1762019304
Allocated memory in use = 100133944
Free memory = 1762137032

----- fragmented memory statistics -----
fragment size count total (bytes) fragment size count total (bytes)
------------------------------- --------------- ------------------------ ------------------------
32768 1 33176
1762019304 1 1762019304*

----- allocated memory statistics -----
fragment size count total (bytes) fragment size count total (bytes)
------------------------------- --------------- ------------------------ ------------------------
49152 10 491520
65536 125 8192000
98304 3 294912
131072 18 2359296

> show memory binsize 131072
MEMPOOL_DMA pool bin stats:
MEMPOOL_GLOBAL_SHARED pool bin stats:
```

The following output confirms that a block of size 150,000 was allocated, instead of 131,072:

```
> show memory binsize 131072
MEMPOOL_DMA pool bin stats:
MEMPOOL_GLOBAL_SHARED pool bin stats:
```
The approximate number of total bytes shown in the show memory detail command output is by design. There are two reasons for this:

- For each fragment size, if you had to get the sum of all fragments, a performance impact would occur because there can be very large number of allocations for a single fragment size and to get the accurate value, you need to walk over thousands of chunks.

- For each binsize, you need to walk through the doubly linked list of allocations and there could be many allocations. In this case, you cannot hog the CPU for an extended period and would need to suspend allocations periodically. After you resume allocations, other processes may have allocated or deallocated memory and memory states may have changed. As a result, the total bytes column gives an approximate value instead of the real value.

Examples

The following is sample output from the show memory command:

```
> show memory
Free memory: 2986716635 bytes (64%)
Used memory: 1646723072 bytes (36%)
------------------ ------------------
Total memory: 4633439707 bytes (100%)
```

Note: Free memory is the free system memory. Additional memory may be available from memory pools internal to the ASA process. Use 'show memory detail' to see this information, but use it with care since it may cause CPU hogs and packet loss under load.

```
> show memory system
Mem: 3982640 3014544 240200 0 159932 567964
-/+ buffers/cache: 3014544 968096
Swap: 3998716 137704 3861012
```

The following example shows how to display system-level memory usage.

The following is sample output from the show memory detail command:

```
> show memory detail
Heap Memory:
  Free Memory:
```
<table>
<thead>
<tr>
<th>Memory Pool</th>
<th>Used Memory</th>
<th>System Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heapcache Pool</td>
<td>3804848 bytes (0%)</td>
<td>2986716635 bytes (64%)</td>
</tr>
<tr>
<td>Global Shared Pool</td>
<td>67372768 bytes (1%)</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>4633439707 bytes (100%)</td>
<td></td>
</tr>
</tbody>
</table>

**Used Memory:**

- **Heapcache Pool:** 308670800 bytes (7%)
- **Global Shared Pool:** 6432 bytes (0%)
- **Reserved (Size of DMA Pool):** 499122176 bytes (11%)
- **Reserved for messaging:** 2097152 bytes (0%)
- **System Overhead:** 765648896 bytes (17%)

---

**Total Memory:** 4633439707 bytes (100%)

Warning: The information reported here is computationally expensive to determine, and may result in CPU hogs and performance impact.

---

**MEMPOOL_MSLGKR POOL STATS:**

- Non-mmapped bytes allocated: 2097152
- Number of free chunks: 1
- Number of mmapped regions: 0
- Mmapped bytes allocated: 0
- Max memory footprint: 2097152
- Keepcost: 2092768
- Max contiguous free mem: 2092768
- Allocated memory in use: 4288
- Free memory: 2092864

----- fragmented memory statistics -----

(...Remaining output truncated...)

The following example shows the chunks allocated to bin size 8192.

```bash
> show memory binsize 8192
MEMPOOL_HEAPCACHE_0 pool bin stats:
pc = 0x7efc3f80e508, size = 773406, count = 92
pc = 0x7efc3e3c5013, size = 189152, count = 23
pc = 0x7efc405df64f, size = 287036, count = 32
pc = 0x7efc3f9ef622, size = 8128, count = 1
pc = 0x7efc3f4fd5f5, size = 871744, count = 106
pc = 0x7efc3f4fd8b7, size = 82240, count = 10
pc = 0x7efc3f18c3e6, size = 20272, count = 2
pc = 0x7efc3f557139, size = 8192, count = 1
pc = 0x7efc3e1f1697, size = 8344, count = 1
pc = 0x7efc3e0506f6, size = 8192, count = 1
MEMPOOL_DMA pool bin stats:
pc = 0x7efc3e1lcca68, size = 10240, count = 1
MEMPOOL_GLOBAL_SHARED pool bin stats:
```

This following example is sample output from the `show memory api` command. It shows that the memory tracker and delayed-free-poisoner memory features are active.

```bash
> show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

The following example shows how to display system-level memory usage.
### show memory

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show memory profile</td>
<td>Displays information about the memory usage (profiling) of the Firepower Threat Defense.</td>
</tr>
</tbody>
</table>
show memory delayed-free-poisoner

To display a summary of the memory delayed-free-poisoner queue usage, use the show memory delayed-free-poisoner command.

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

Use the memory delayed-free-poisoner enable command to enable the feature. Use the clear memory delayed-free-poisoner command to clear the queue and statistics.

## Examples

This following is sample output from the show memory delayed-free-poisoner command:

```
> memory delayed-free-poisoner enable
> show memory delayed-free-poisoner

delayed-free-poisoner settings:
delayed-free-poisoner threshold 100
delayed-free-poisoner desired-fragment-size 102400
delayed-free-poisoner desired-fragment-count 16
delayed-free-poisoner watchdog-percent 50

delayed-free-poisoner statistics:
136064: current memory in queue
500: current queue length
0: frees dequeued
280: frees not queued for size
0: frees not queued for locking
0: successful validate runs
0: aborted validate runs
never: time of last validate
0: threshold defragment operations
0: size and/or count defragment operations
0: watchdog-aborts
```
show memory logging

To display memory usage logging, use the `show memory logging` command.

```
show memory logging  [ wrap  |  brief  |  include  [ option ] ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>(Optional) Displays abbreviated memory usage logging.</td>
</tr>
<tr>
<td>include option</td>
<td>(Optional) Includes only the specified fields in the output. You can specify the keywords for the fields in any order, but they always appear in the following order. If you do not include an option, the output is the same as if you had specified <code>brief</code> instead of <code>include</code>.</td>
</tr>
<tr>
<td>wrap</td>
<td>(Optional) Displays memory usage logging wrapped data, which is purged after you enter this command so that duplicate data does not appear and is not saved.</td>
</tr>
</tbody>
</table>

- process
- time
- operator (free/malloc/etc.)
- address
- size
- callers

The output format is:

```
process=[XXX] time=[XXX] oper=[XXX] address=0xXXXXXXXXX size=XX @ XXXXXXXXXX
```

Up to four caller addresses appear. The types of operations are listed in the output (Number of...) shown in the example.

**Command History**

```
Release  Modification
6.1      This command was introduced.
```

**Usage Guidelines**

Use the `show memory logging` command to view memory log information. You must first enable this logging using the `memory logging` command.

**Examples**

The following is sample output from the `show memory logging` command.

```
> memory logging 1024
> show memory logging
Number of free 203989
Number of calloc 83703
```
The following is sample output from the show memory logging brief command.

```
show memory logging brief
Number of free 223195
Number of calloc 91624
Number of malloc 131572
Number of realloc-new 0
Number of realloc-free 0
Number of realloc-null 0
Number of realloc-same 0
Number of calloc-fail 0
Number of malloc-fail 0
Number of realloc-fail 0
Total operations 446391
Buffer size: 1024 (73816 x2 bytes)
```
show memory profile

To display information about the memory usage (profiling) of the Firepower Threat Defense device, use the `show memory profile` command.

```
show memory profile  [status  |  peak  [detail  |  collated ]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>collated</td>
<td>(Optional) Collates the memory information displayed.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed memory information.</td>
</tr>
<tr>
<td>peak</td>
<td>(Optional) Displays the peak capture buffer rather than the “in use” buffer.</td>
</tr>
<tr>
<td>status</td>
<td>(Optional) Displays the current state of memory profiling and the peak capture buffer.</td>
</tr>
</tbody>
</table>

**Command History**

```
Release   | Modification
----------|----------------
6.1       | This command was introduced.
```

**Usage Guidelines**

Use the `show memory profile` command to troubleshoot memory usage level and memory leaks. You can still see the profile buffer contents even if profiling has been stopped. Starting profiling clears the buffer automatically.

**Note**

The Firepower Threat Defense device might experience a temporary reduction in performance when memory profiling is enabled.

**Examples**

The following is sample output from the `show memory profile` command:

```
> show memory profile
Range: start = 0x0004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

The output of the `show memory profile detail` command is divided into six data columns and one header column, at the far left. The address of the memory bucket corresponding to the first data column is given at the header column (the hexadecimal number). The data itself is the number of bytes that is held by the text/code that falls in the bucket address. A period (.) in the data column means no memory is held by the text at this bucket. Other columns in the row correspond to the bucket address that is greater than the increment amount from the previous column. For example, the address bucket of the first data column in the first row is 0x001069e0. The address bucket of the second data column in the first row is 0x001069e4 and so on. Normally the header column address is the next bucket address; that is, the address of the last data column of the previous row plus the increment. All rows without any usage are suppressed. More than one such contiguous row can be suppressed, indicated with three periods at the header column (...).
The following is sample output from the `show memory profile peak detail` command, which shows the peak capture buffer and the number of bytes that is held by the text/code that falls in the corresponding bucket address:

```plaintext
> show memory profile peak detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 24462 . . . .
...
0x00106d88 1865870 . . . .
...
0x0010adf0 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . .
(...output truncated...)
```

The following is sample output from the `show memory profile peak collated` command:

```plaintext
> show memory profile peak collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<More>
```

The following is sample output from the `show memory profile peak` command, which shows the peak capture buffer:

```plaintext
> show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

The following is sample output from the `show memory profile status` command, which shows the current state of memory profiling and the peak capture buffer:

```plaintext
> show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

---

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory profile enable</td>
<td>Enables the monitoring of memory usage (memory profiling).</td>
</tr>
<tr>
<td>memory profile text</td>
<td>Configures a program text range of memory to profile.</td>
</tr>
<tr>
<td>clear memory profile</td>
<td>Clears the memory buffers held by the memory profiling function.</td>
</tr>
</tbody>
</table>
show memory tracking

To display currently allocated memory tracked by the tool, use the `show memory tracking` command.

```
show memory tracking [address | detail | dump tracked_address]
```

**Syntax Description**

- **address** (Optional) Shows memory tracking by address.
- **detail** (Optional) Shows the internal memory tracking state.
- **dump tracked_address** (Optional) Shows the dump of the specified memory tracking address, 0-4294967295.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show memory tracking` command to show currently allocated memory tracked by the tool. You must use `memory tracking enable` before you can see this information.

**Examples**

The following is sample output from the `show memory tracking` command:

```
> show memory tracking
memory tracking by caller:
  bytes-threshold: 0
  allocates-by-threshold: 0
  65406 bytes from 49 allocates by 0x00007efc3f80e508
  3000 bytes from 1 allocates by 0x00007efc3f4e1278
  159 bytes from 1 allocates by 0x00007efc3fe9ee13
  17 bytes from 1 allocates by 0x00007efc3fe9ef4e
```

The following is sample output from the `show memory tracking address` command:

```
> show memory tracking address
memory tracking by caller:
  bytes-threshold: 0
  allocates-by-threshold: 0
  58918 bytes from 49 allocates by 0x00007efc3f80e508
  3000 bytes from 1 allocates by 0x00007efc3f4e1278
  167 bytes from 1 allocates by 0x00007efc3fe9ee13
  17 bytes from 1 allocates by 0x00007efc3fe9ef4e
memory tracking address pool:
  32 byte region @ 0x00007efc358a06e0 allocated by 0x00007efc3f80e508
  96 byte region @ 0x00007efc351d0880 allocated by 0x00007efc3f80e508
  896 byte region @ 0x00007efc35f121c0 allocated by 0x00007efc3f80e508
  8192 byte region @ 0x00007efc35832e20 allocated by 0x00007efc3f80e508
  96 byte region @ 0x00007efc30483910 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc359e3960 allocated by 0x00007efc3f80e508
  1036 byte region @ 0x00007efc35f04680 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc36024890 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc35fd48a0 allocated by 0x00007efc3f80e508
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear memory tracking</td>
<td>Clears all currently collected information.</td>
</tr>
<tr>
<td>memory tracking</td>
<td>Enables memory tracking.</td>
</tr>
</tbody>
</table>

---

32 byte region @ 0x00007efc35f04ad0 allocated by 0x00007efc3f90e508
34 byte region @ 0x00007efc35e54e00 allocated by 0x00007efc3f90e508
8192 byte region @ 0x00007efc35f83e70 allocated by 0x00007efc3f90e508
40 byte region @ 0x00007efc36005cc0 allocated by 0x00007efc3f90e508
11 byte region @ 0x00007efc360061e0 allocated by 0x00007efc3f90e508
76 byte region @ 0x00007efc35f7a6d0 allocated by 0x00007efc3f90e508
1024 byte region @ 0x00007efc35f8574f0 allocated by 0x00007efc3f90e508
8 byte region @ 0x00007efc365b7e0 allocated by 0x00007efc3f90e508
56 byte region @ 0x00007efc365b7f90 allocated by 0x00007efc3f90e508
168 byte region @ 0x00007efc365b8210 allocated by 0x00007efc3f90e508
112 byte region @ 0x00007efc365b8300 allocated by 0x00007efc3f90e508
112 byte region @ 0x00007efc365b83c0 allocated by 0x00007efc3f90e508
16 byte region @ 0x00007efc365b8560 allocated by 0x00007efc3f90e508
16 byte region @ 0x00007efc365b85c0 allocated by 0x00007efc3f90e508
112 byte region @ 0x00007efc365b8610 allocated by 0x00007efc3f90e508
88 byte region @ 0x00007efc365f7a8e0 allocated by 0x00007efc3f90e508
8 byte region @ 0x00007efc365f7a8e60 allocated by 0x00007efc3f90e508
4112 byte region @ 0x00007efc35f7a90c0 allocated by 0x00007efc3f90e508
17 byte region @ 0x00007efc365b95a0 allocated by 0x00007efc3f90e508
72 byte region @ 0x00007efc365b9600 allocated by 0x00007efc3f90e508
72 byte region @ 0x00007efc365b9690 allocated by 0x00007efc3f90e508
72 byte region @ 0x00007efc365b9720 allocated by 0x00007efc3f90e508
40 byte region @ 0x00007efc365b97b0 allocated by 0x00007efc3f90e508
24 byte region @ 0x00007efc365b9820 allocated by 0x00007efc3f90e508
2 byte region @ 0x00007efc365b9880 allocated by 0x00007efc3f90e508
76 byte region @ 0x00007efc35f7a9aa0 allocated by 0x00007efc3f90e508
776 byte region @ 0x00007efc35f7a9fa0 allocated by 0x00007efc3f90e508
512 byte region @ 0x00007efc365f7a0080 allocated by 0x00007efc3f90e508
936 byte region @ 0x00007efc35f7a9a80 allocated by 0x00007efc3f90e508
24 byte region @ 0x00007efc365f7a290 allocated by 0x00007efc3f90e508
568 byte region @ 0x00007efc35f7a2c40 allocated by 0x00007efc3f90e508
512 byte region @ 0x00007efc35f7a38a0 allocated by 0x00007efc3f90e508
40 byte region @ 0x00007efc35f7a3e0 allocated by 0x00007efc3f90e508
1665 byte region @ 0x00007efc35f7a3a0 allocated by 0x00007efc3f90e508
16 byte region @ 0x00007efc35f7a5f0 allocated by 0x00007efc3f90e508
112 byte region @ 0x00007efc35f7a6e0 allocated by 0x00007efc3f90e508
4112 byte region @ 0x00007efc35f7a6e0 allocated by 0x00007efc3f90e508
4112 byte region @ 0x00007efc35f7a6e0 allocated by 0x00007efc3f90e508
8208 byte region @ 0x00007efc35f7a6e0 allocated by 0x00007efc3f90e508
386 byte region @ 0x00007efc35f7a6e0 allocated by 0x00007efc3f90e508
72 byte region @ 0x00007efc35f7a6e0 allocated by 0x00007efc3f90e508
8208 byte region @ 0x00007efc35f7a6e0 allocated by 0x00007efc3f90e508
4112 byte region @ 0x00007efc35f7a6e0 allocated by 0x00007efc3f90e508
3000 byte region @ 0x00007efc35f7a6e0 allocated by 0x00007efc3f90e508
32 byte region @ 0x00007efc35f7a6e0 allocated by 0x00007efc3f90e508
16 byte region @ 0x00007efc35f7a790 allocated by 0x00007efc3f90e508
1036 byte region @ 0x00007efc35f7a808 allocated by 0x00007efc3f90e508
512 byte region @ 0x00007efc35f7a808 allocated by 0x00007efc3f90e508
360 byte region @ 0x00007efc35f7a808 allocated by 0x00007efc3f90e508
24 byte region @ 0x00007efc35f7a808 allocated by 0x00007efc3f90e508
show memory webvpn

To generate memory usage statistics for WebVPN, use the `show memory webvpn` command.

```
show memory webvpn [allobjects | blocks | dumpstate filename | pools | usedobjects]
show memory webvpn profile [clear | dump filename | start | stop]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>allobjects</code></td>
<td>Displays WebVPN memory consumption details for pools, blocks, and all used and freed objects.</td>
</tr>
<tr>
<td><code>blocks</code></td>
<td>Displays WebVPN memory consumption details for memory blocks.</td>
</tr>
<tr>
<td><code>clear</code></td>
<td>Clears the WebVPN memory profile.</td>
</tr>
<tr>
<td><code>dump filename</code></td>
<td>Puts WebVPN memory profile into the specified file. The file name should include the location, which can be disk0:, disk1:, flash:, ftp:, tftp:.</td>
</tr>
<tr>
<td><code>dumpstate filename</code></td>
<td>Puts WebVPN memory state into the specified file. The file name should include the location, which can be disk0:, disk1:, flash:, ftp:, tftp:.</td>
</tr>
<tr>
<td><code>pools</code></td>
<td>Shows WebVPN memory consumption details for memory pools.</td>
</tr>
<tr>
<td><code>profile</code></td>
<td>Obtains the WebVPN memory profile and places it in a file.</td>
</tr>
<tr>
<td><code>start</code></td>
<td>Starts gathering the WebVPN memory profile.</td>
</tr>
<tr>
<td><code>stop</code></td>
<td>Stops getting the WebVPN memory profile.</td>
</tr>
<tr>
<td><code>usedobjects</code></td>
<td>Displays WebVPN memory consumption details for used objects.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show memory webvpn allobjects` command:

```
> show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" -> "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719a20..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd709ff8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
```
show memory webvpn

Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0x070b50: FREED (by "jvclass_pool_free")
show mfib

To display information from the Multicast Forwarding Information Base, use the `show mfib` command.

```
show mfib [source_or_group [group]] [cluster | count | verbose]
show mfib [active [kbps] | cluster-stats | interface | status | summary]
show mfib reserved [active [kbps] | cluster | count | verbose]
```

**Syntax Description**

- `[active [kbps]]` (Optional) Displays active multicast sources. You can specify a kilobit per second limit the display to multicast streams that are greater-than or equal to this value. The default is 4, the range is 0-4294967295.
- `cluster` (Optional) Displays the MFIB epoch number and the current timer value. You cannot specify `cluster` if you specify both a source and group.
- `cluster-stats` (Optional) Displays MFIB cluster synchronization statistics.
- `count` (Optional) Displays MFIB route and packet count data. This command displays packet drop statistics.
- `interface` (Optional) Displays packet statistics for interfaces that are related to the MFIB process.
- `reserved` (Optional) Displays MFIB entries for reserved groups, in the range 224.0.0.0 through 224.0.0.225.
- `source_or_group [group]` (Optional) The source or group IPv4, IPv6, or name. If you specify both, specify the source first. The source address is a unicast address.
- `status` (Optional) Displays the general MFIB configuration and operational status.
- `summary` (Optional) Displays summary information about the number of MFIB entries and interfaces.
- `verbose` (Optional) Displays detail information about the forwarding entries and interfaces.

**Command Default**

Without the optional arguments, information for all groups is shown.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show mfib` command:

```
> show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
```
The following is sample output from the `show mfib verbose` command:

```
> show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
        AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
        IC - Internal Copy, NP - Not platform switched
        SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
    Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
    Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
    Forwarding: 0/0/0/0, Other: 0/0/0
```

The following sample output from the `show mfib count` command:

```
> show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

The following is sample output from the `show mfib active` command. The output displays either positive or negative numbers for the rate PPS. The command displays negative numbers when RPF packets fail or when the router observes RPF packets with an interfaces out (OIF) list. This type of activity may indicate a multicast routing problem.

```
> show mfib active
Active IP Multicast Sources - sending >= 4 kbps
Group: 224.2.127.254, (sdr.cisco.com)
    Source: 192.168.28.69 (mbone.ipd.anl.gov)
    Rate: 1 pps/4 kbps (1sec), 4 kbps (last 1 secs), 4 kbps (life avg)
Group: 224.2.201.241, ACM 97
    Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
    Rate: 9 pps/93 kbps (1sec), 145 kbps (last 20 secs), 85 kbps (life avg)
Group: 224.2.207.215, ACM 97
    Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
    Rate: 3 pps/31 kbps (1sec), 63 kbps (last 19 secs), 65 kbps (life avg)
```

The following example is sample output from the `show mfib interface` command:
show mfib interface

IP Multicast Forwarding (MFIB) status:
  Configuration Status: enabled
  Operational Status: running

<table>
<thead>
<tr>
<th>MFIB interface</th>
<th>status CEF-based output [configured,available]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0</td>
<td>up [no, no]</td>
</tr>
<tr>
<td>Ethernet1</td>
<td>up [no, no]</td>
</tr>
<tr>
<td>Ethernet2</td>
<td>up [no, no]</td>
</tr>
</tbody>
</table>

The following is sample output from the `show mfib status` command:

> show mfib status

IP Multicast Forwarding (MFIB) status:
  Configuration Status: enabled
  Operational Status: running

The following is sample output from the `show mfib summary` command:

> show mfib summary

IPv6 MFIB summary:

54  total entries [1 (S,G), 7 (*.G), 46 (*.G/m)]
17  total MFIB interfaces

The following is sample output from the `show mfib reserved` command:

> show mfib reserved

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag, AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(*,224.0.0.0/4) Flags: C K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
  Forwarding: 0/0/0/0, Other: 0/0/0
outside Flags: IC
dmz Flags: IC
inside Flags: IC

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mfib counters</td>
<td>Clears MFIB router packet counters.</td>
</tr>
<tr>
<td>show mroute active</td>
<td>Displays active multicast streams.</td>
</tr>
<tr>
<td>show mroute count</td>
<td>Displays multicast route counters.</td>
</tr>
<tr>
<td>show mroute summary</td>
<td>Displays multicast routing table summary information.</td>
</tr>
</tbody>
</table>
**show mgcp**

To display Media Gateway Control Protocol (MGCP) configuration and session information, use the `show mgcp` command.

```
show mgcp {commands | sessions} [detail]
```

**Syntax Description**

- **commands**
  - Lists the number of MGCP commands in the command queue.

- **detail**
  - (Optional) Lists additional information about each command or session in the output.

- **sessions**
  - Lists the number of existing MGCP sessions.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To display MGCP information, you must inspect MGCP traffic. To inspect MGCP traffic, you need to configure a FlexConfig in Firepower Management Center.

**Example**

The following are examples of the `show mgcp` command options:

```
> show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07

> show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
  Gateway IP | host-pc-2
  Transaction ID 2052
  Endpoint name | aaln/1
  Call ID | 9876543210abcdef
  Connection ID |
  Media IP | 192.168.5.7
  Media port | 6058

> show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11

> show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
  Gateway IP | host-pc-2
  Call ID | 9876543210abcdef
  Connection ID | 6789af54c9
  Endpoint name | aaln/1
  Media lcl port 6166
  Media rmt IP | 192.168.5.7
```
Media rmt port 6058
show mode

To show the security context mode for the system, use the show mode command.

```
show mode
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The Firepower Threat Defense device supports single context only. Multiple context mode is not supported.

### Examples

The following example shows how to display the security context mode.

```
> show mode
Security context mode: single
```
**show model**

To display the hardware model of the device, use the `show model` command.

```
show model
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the device model.

```
> show model
Cisco ASA5516-X Threat Defense
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show serial-number</td>
<td>Show the device serial number.</td>
</tr>
<tr>
<td>show version</td>
<td>Show software and other device version information.</td>
</tr>
</tbody>
</table>
show module

To show information about a module installed on the Firepower Threat Defense device, use the `show module` command in user EXEC mode.

```
show module [id [details | recover | log console]] | all]
```

**Syntax Description**

- **all** *(Default)* Shows information for all modules. This is the default.
- **details** *(Optional)* Shows additional information, including remote management configuration for modules.
- **id** Specifies the module ID. Use show module without parameters to see the available slot numbers, which are typically 0 and 1.
- **log console** *(Optional)* Shows log information for the module. This option might not be valid for every module.
- **recover** *(Optional)* Shows the settings for recovering the module.

**Command Default**

By default, information for all modules is shown.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command shows information about the modules installed in the Firepower Threat Defense device. The Firepower Threat Defense itself also appears as a module in the display (in slot 0). Whether a device supports additional modules differs by device model.

The output of the `show module details` command varies according to which module is installed.

For models that allow you to configure software modules, the `show module` command lists all possible modules. Status information indicates whether one of them is installed.

**Examples**

The following sample output is for an ASA 5516-X running Firepower Threat Defense software. For this device, it is normal for slot 1 to be unknown, because Firepower Threat Defense does not support any software modules.

```
> show module

<table>
<thead>
<tr>
<th>Mod</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ASA 5516-X with FirePOWER services, 8GE, AC, ASA5516</td>
<td>JAD19390561</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Unknown</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>MAC Address Range</th>
<th>Hw Version</th>
<th>Fw Version</th>
<th>Sw Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>84b2.61b1.92be to 84b2.61b1.92c6</td>
<td>1.0</td>
<td>1.1.3</td>
<td>97.1(0)60</td>
</tr>
<tr>
<td>1</td>
<td>84b2.61b1.92bd to 84b2.61b1.92bd</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Mod</th>
<th>SSM Application Name</th>
<th>Status</th>
<th>SSM Application Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unknown</td>
<td>No Image Present</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>Status</th>
<th>Data Plane Status</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Up Sys</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Unresponsive</td>
<td>Not Applicable</td>
<td></td>
</tr>
</tbody>
</table>

The following table describes each field listed in the output.

**Table 46: show module Output Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mod</td>
<td>The module number, 0 or 1.</td>
</tr>
<tr>
<td>Card Type</td>
<td>The card type. For the device shown in module 0, the type is the platform model. For slot 1, it would be the extra module, if any.</td>
</tr>
<tr>
<td>Model</td>
<td>The model number for this module.</td>
</tr>
<tr>
<td>Serial No.</td>
<td>The serial number.</td>
</tr>
<tr>
<td>MAC Address Range</td>
<td>The MAC address range for interfaces on this module.</td>
</tr>
<tr>
<td>Hw Version</td>
<td>The hardware version.</td>
</tr>
<tr>
<td>Fw Version</td>
<td>The firmware version.</td>
</tr>
<tr>
<td>Sw Version</td>
<td>The software version. This is not the Firepower Threat Defense version. Instead, it is an ASA software version, which is a component of Firepower Threat Defense software. Use the <code>show version</code> command to see the Firepower Threat Defense version.</td>
</tr>
<tr>
<td>SSM Application Name</td>
<td>The name of the application running on the security services module.</td>
</tr>
<tr>
<td>SSM Application Version</td>
<td>The version of the application running on the security services module.</td>
</tr>
</tbody>
</table>
For the device in module 0, the status is Up Sys. The status of the module in slot 1 can be any of the following:

- Initializing—The module is being detected and the control communication is being initialized by the device.
- Up—The module has completed initialization by the device.
- Unresponsive—The device encountered an error while communicating with this module.
- Reloading—The module is reloading.
- Shutting Down—The module is shutting down.
- Down—The module is shut down.
- Recover—The module is attempting to download a recovery image.
- No Image Present—The module software has not been installed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>For the device in module 0, the status is Up Sys. The status of the module in slot 1 can be any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Initializing—The module is being detected and the control communication is being initialized by the device.</td>
</tr>
<tr>
<td></td>
<td>• Up—The module has completed initialization by the device.</td>
</tr>
<tr>
<td></td>
<td>• Unresponsive—The device encountered an error while communicating with this module.</td>
</tr>
<tr>
<td></td>
<td>• Reloading—The module is reloading.</td>
</tr>
<tr>
<td></td>
<td>• Shutting Down—The module is shutting down.</td>
</tr>
<tr>
<td></td>
<td>• Down—The module is shut down.</td>
</tr>
<tr>
<td></td>
<td>• Recover—The module is attempting to download a recovery image.</td>
</tr>
<tr>
<td></td>
<td>• No Image Present—The module software has not been installed.</td>
</tr>
<tr>
<td>Data Plane Status</td>
<td>The current state of the data plane.</td>
</tr>
<tr>
<td>Compatibility</td>
<td>The compatibility of the module relative to the rest of the device.</td>
</tr>
</tbody>
</table>
show monitor-interface

To display information about the interfaces monitored for failover, use the show monitor-interface command.

show monitor-interface

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Because an interface can have more than one IPv6 address configured on it, only the link-local address is displayed in the show monitor-interface command. If both IPv4 and IPv6 addresses are configured on an interface, both addresses appear in the output. If there is no IPv4 address configured on the interface, the IPv4 address in the output appears as 0.0.0.0. If there is no IPv6 address configured on an interface, the address is simply omitted from the output.

Monitored failover interfaces can have the following status:

- (Waiting) coupled with any other status, such as Unknown (Waiting)—The interface has not yet received a hello packet from the corresponding interface on the peer unit.
- Unknown—Initial status. This status can also mean the status cannot be determined.
- Normal—The interface is receiving traffic. If the status is Normal (Waiting), verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
- Testing—Hello messages are not heard on the interface for five poll times.
- Link Down—The interface or VLAN is administratively down.
- No Link—The physical link for the interface is down.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

Examples

The following is sample output from the show monitor-interface command:

```bash
> show monitor-interface
This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```
show mrib client

To display information about the MRIB client connections, use the `show mrib client` command.

```
show mrib client  [filter]  [name  client_name]
```

**Syntax Description**

- **filter**  
  (Optional) Displays client filter. Used to view information about the MRIB flags that each client owns and the flags in which each client is interested.

- **name client_name**  
  (Optional) Name of a multicast routing protocol that acts as a client of MRIB, such as PIM or IGMP.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `filter` option is used to display the route and interface level flag changes that various MRIB clients have registered. This command option also shows what flags are owned by the MRIB clients.

**Examples**

The following sample output from the `show mrib client` command using the `filter` keyword:

```
> show mrib client filter
MFWD:0 (connection id 0)
  interest filter:
  entry attributes: S C IA D
  interface attributes: F A IC NS DP SP
  groups:
  include 0.0.0.0/0
  interfaces:
  include All
  ownership filter:
  groups:
  include 0.0.0.0/0
  interfaces:
  include All
  igmp:77964 (connection id 1)
  ownership filter:
  interface attributes: II ID LI LD
  groups:
  include 0.0.0.0/0
  interfaces:
  include All
  pim:49287 (connection id 5)
  interest filter:
  entry attributes: E
  interface attributes: SP II ID LI LD
  groups:
  include 0.0.0.0/0
  interfaces:
  include All
  ownership filter:
  entry attributes: L S C IA D
```
interface attributes: F A IC NS DF

groups:
include 0.0.0.0/0

interfaces:
include All

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mrib route</td>
<td>Displays MRIB table entries.</td>
</tr>
</tbody>
</table>
show mrib route

To display entries in the MRIB table, use the `show mrib route` command.

```
show mrib route  [[ [source  | *] [group [/prefix-length]] ] | summary]
```

**Syntax Description**

- `*` (Optional) Display shared tree entries.
- `/prefix-length` (Optional) Prefix length of the MRIB route. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- `group` (Optional) IP address or name of the group.
- `source` (Optional) IP address or name of the route source.
- `summary` Displays a summary of the MRIB table entries.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The MFIB table maintains a subset of entries and flags updated from MRIB. The flags determine the forwarding and signaling behavior according to a set of forwarding rules for multicast packets.

In addition to the list of interfaces and flags, each route entry shows various counters. Byte count is the number of total bytes forwarded. Packet count is the number of packets received for this entry. The `show mfib count` command displays global counters independent of the routes.

**Examples**

The following is sample output from the `show mrib route` command:

```
> show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
             C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
                NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
                II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
                Decapstunnel0 Flags: NS
(*,224.0.0.0/24) Flags: D
(*,224.0.1.39) Flags: S
(*,224.0.1.40) Flags: S
POS0/3/0/0 Flags: II LI
(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
                POS0/3/0/0 Flags: F NS LI
```

Cisco Firepower Threat Defense Command Reference
Decapstunne10 Flags: A
(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
POS0/3/0/0 Flags: F NS
Decapstunne10 Flags: A

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib count</td>
<td>Displays route and packet count data for the MFIB table.</td>
</tr>
</tbody>
</table>
show mroute

To display the IPv4 multicast routing table, use the `show mroute` command.

```
show mroute [group [source] | reserved] [active [rate] | count | pruned | summary]
```

**Syntax Description**

- **active rate** (Optional) Displays only active multicast sources. Active sources are those sending at the specified rate or higher. If the rate is not specified, active sources are those sending at a rate of 4 kbps or higher.
- **count** (Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
- **group** (Optional) IP address or name of the multicast group as defined in the DNS hosts table.
- **pruned** (Optional) Displays pruned routes.
- **reserved** (Optional) Displays reserved groups.
- **source** (Optional) Source hostname or IP address.
- **summary** (Optional) Displays a one-line, abbreviated summary of each entry in the multicast routing table.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show mroute` command displays the contents of the multicast routing table. The device populates the multicast routing table by creating (S,G) and (*,G) entries based on PIM protocol messages, IGMP reports, and traffic. The asterisk (*) refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (through RPF).

To view the `mroute` commands in the running configuration, use the `show running-config mroute` command.

**Examples**

The following is sample output from the `show mroute` command:

```
> show mroute
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
   C - Connected, L - Local, I - Received Source Specific Host Report,
   P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
   J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
```
Incoming interface: Null
RPF nbr: 0.0.0.0
Outgoing interface list:
  inside, Null, 08:05:45/never
tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
Incoming interface: outside
RPF nbr: 140.0.0.70
Outgoing interface list:
  inside, Forward, 08:07:44/never

The following fields are shown in the `show mroute` output:

- **Flags**—Provides information about the entry.
  - D—Dense. Entry is operating in dense mode.
  - S—Sparse. Entry is operating in sparse mode.
  - B—Bidir Group. Indicates that a multicast group is operating in bidirectional mode.
  - s—SSM Group. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.
  - C—Connected. A member of the multicast group is present on the directly connected interface.
  - L—Local. The device itself is a member of the multicast group. Groups are joined locally by the igmp join-group command (for the configured group).
  - I—Received Source Specific Host Report. Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by IGMP. This flag is set only on the DR.
  - P—Pruned. Route has been pruned. The software keeps this information so that a downstream member can join the source.
  - R—RP-bit set. Indicates that the (S, G) entry is pointing toward the RP.
  - F—Register flag. Indicates that the software is registering for a multicast source.
  - T—SPT-bit set. Indicates that packets have been received on the shortest path source tree.
  - J—Join SPT. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the device to join the source tree.

For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the device monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute.
The device measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J-Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.

If the default SPT-Threshold value of 0 kbps is used for the group, the J-Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the device immediately switches to the shortest path source tree when traffic from a new source is received.

- **Timers: Uptime/Expires**—Uptime indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. Expires indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.

- **Interface state**—Indicates the state of the incoming or outgoing interface.
  - **Interface**—The interface name listed in the incoming or outgoing interface list.
  - **State**—Indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists or a time-to-live (TTL) threshold.

- **(*, 239.1.1.40) and (*, 239.2.2.1)**—Entries in the IP multicast routing table. The entry consists of the IP address of the source followed by the IP address of the multicast group. An asterisk (*) in place of the source indicates all sources.

- **RP**—Address of the RP. For routers and access servers operating in sparse mode, this address is always 224.0.0.0.

- **Incoming interface**—Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.

- **RPF nbr**—IP address of the upstream router to the source.

- **Outgoing interface list**—Interfaces through which packets will be forwarded.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config mroute</td>
<td>Displays configured multicast routes.</td>
</tr>
</tbody>
</table>
show nameif

To view the logical name for an interface, use the **show nameif** command.

**show nameif**  *[physical_interface [subinterface] | zone]*

### Syntax Description

- **physical_interface**: (Optional) Identifies the interface ID, such as `gigabitethernet0/1`.
- **subinterface**: (Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
- **zone**: (Optional) Shows the zone and inline set names.

### Command Default

If you do not specify an interface, this command displays all interface names.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to show the names assigned to the interfaces. An interface must be named to use it in any configuration setting. It also shows the security level for the interface, which is always 0 for Firepower Threat Defense.

If you add the **zone** keyword, the Zone Name column indicates the inline set or traffic zone to which the interface belongs. Traffic zone is not the same as security zone, so if you do not have passive interfaces or inline sets, the column might be empty even though the interfaces belong to routed or switched security zones. Use the device manager to determine which security zones contain each interface.

### Examples

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

```
> show nameif
Interface     Name     Security
GigabitEthernet1/1 outside  0
GigabitEthernet1/2 insidel_2  0
GigabitEthernet1/3 insidel_3  0
GigabitEthernet1/4 insidel_4  0
GigabitEthernet1/5 insidel_5  0
GigabitEthernet1/6 insidel_6  0
GigabitEthernet1/7 insidel_7  0
GigabitEthernet1/8 insidel_8  0
Management1/1 diagnostic  0
BVI1 inside  0
```

The following is sample output that shows zone membership. In this example, 2 interfaces are in inline sets, and one interface is in a passive traffic zone.

```
> show nameif zone
Interface     Name     Zone Name     Security
GigabitEthernet0/0 passive passive-security-zone  0
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>IS-IS ID</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/1</td>
<td>in</td>
<td>is-154</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet0/2</td>
<td>out</td>
<td>is-154</td>
<td>0</td>
</tr>
<tr>
<td>Management0/0</td>
<td>diagnostic</td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>
**show nat**

To display statistics of NAT policies, use the **show nat** command.

```
show nat [interface name] [ip_addr [mask] | {object | object-group} name] [translated [interface name] [ip_addr [mask] | {object | object-group} name]] [detail]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Includes more verbose expansion of the object fields.</td>
</tr>
<tr>
<td>interface name</td>
<td>(Optional) Specifies the source interface.</td>
</tr>
<tr>
<td>ip_addr [mask]</td>
<td>(Optional) Specifies an IP address and subnet mask.</td>
</tr>
<tr>
<td>object name</td>
<td>(Optional) Specifies a network object or service object.</td>
</tr>
<tr>
<td>object-group name</td>
<td>(Optional) Specifies a network object group</td>
</tr>
<tr>
<td>translated</td>
<td>(Optional) Specifies the translated parameters.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **show nat** command to show runtime representation of the NAT policy. Use the **detail** optional keyword to expand the object and view the object values. Use the additional selector fields to limit the **show nat** command output.

The output shows all NAT commands, even hidden commands. For example, if you configure the management interface to use the data interfaces as a gateway, hidden NAT rules are created for a hidden virtual interface (for example, nlp_int_tap) to enable communications between the management interface and each data interface. These rules are not reflected in the NAT tables in Firepower Device Manager. You will also see hidden rules for any HTTPS/SSH management access rules that allow management connections to data interfaces, which are reflected in the Firepower Device Manager’s management access table but not in the NAT table.

**Examples**

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

```
> show nat
Manual NAT Policies (Section 1)
1 (any) to (any) source dynamic S S' destination static D' D
  translate_hits = 0, untranslate_hits = 0

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic A 2.2.2.2
  translate_hits = 0, untranslate_hits = 0

Manual NAT Policies (Section 3)
1 (any) to (any) source dynamic C C' destination static B' B service R R'
  translate_hits = 0, untranslate_hits = 0
```
show nat detail

Manual NAT Policies (Section 1)
1 (any) to (any) source dynamic S S' destination static D' D
  translate_hits = 0, untranslate_hits = 0
  Source - Real: 1.1.1.2/32, Mapped: 2.2.2.3/32
  Destination - Real: 10.10.10.0/24, Mapped: 20.20.20.0/24

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic A 2.2.2.2
  translate_hits = 0, untranslate_hits = 0
  Source - Real: 1.1.1.1/32, Mapped: 2.2.2.2/32

Manual NAT Policies (Section 3)
1 (any) to (any) source dynamic C C' destination static B' B service R R'
  translate_hits = 0, untranslate_hits = 0
  Source - Real: 11.11.11.10-11.11.11.11, Mapped: 192.168.10.10/32
  Destination - Real: 192.168.1.0/24, Mapped: 10.75.1.0/24
  Service - Real: tcp source eq 10 destination eq ftp-data , Mapped: tcp source eq 100 destination eq 200

The following is sample output from the show nat detail command between IPv6 and IPv4:

show nat detail
1 (in) to (outside) source dynamic inside_nw outside_map destination static inside_map any
  translate_hits = 0, untranslate_hits = 0
  Destination - Origin: 2001::/96, Translated: 0.0.0.0/0

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear nat counters</td>
<td>Clears NAT policy counters.</td>
<td></td>
</tr>
</tbody>
</table>
show nat divert-table

To display statistics of NAT divert table, use the `show nat divert-table` command.

```
show nat divert-table [ipv6] [interface interface_name]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>divert-table</code></td>
<td>Shows the NAT divert table.</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>(Optional) Shows IPv6 entries in the divert table.</td>
</tr>
<tr>
<td><code>interface interface_name</code></td>
<td>(Optional) Limits output to the specified source interface.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show nat divert-table` command to show runtime representation of the NAT divert table. Use the `ipv6` optional keyword to view the IPv6 entries in the divert table. Use the `interface` optional keyword to view the NAT divert table for the specific source interface.

The divert table shows all NAT commands, even hidden commands. For example, if you configure the management interface to use the data interfaces as a gateway, hidden NAT rules are created for a hidden virtual interface (for example, nlp_int_tap) to enable communications between the management interface and each data interface. These rules are not reflected in the NAT tables in Firepower Device Manager.

**Examples**

The following is sample output from the `show nat divert-table` command:

```
> show nat divert-table
Divert Table
id=0xad1521b8, domain=twice-nat section=1 ignore=no
type=none, hits=0, flags=0x9, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
dst ip/id=10.86.119.255, mask=255.255.255.255, port=0-0
input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1523a8, domain=twice-nat section=1 ignore=no
type=none, hits=0, flags=0x9, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
dst ip/id=10.86.116.0, mask=255.255.255.255, port=0-0
input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1865c0, domain=twice-nat section=1 ignore=no
type=none, hits=0, flags=0x9, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad1867b0, domain=twice-nat section=1 ignore=no
type=none, hits=0, flags=0x9, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad257bf8, domain=twice-nat section=1 ignore=no
type=none, hits=0, flags=0x9, protocol=0
```
The following is sample output from the `show nat divert ipv6` command:

```plaintext
> show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear nat counters</code></td>
<td>Clears NAT policy counters.</td>
</tr>
<tr>
<td><code>show nat</code></td>
<td>Displays runtime representation of the NAT policies.</td>
</tr>
</tbody>
</table>
**show nat pool**

To display statistics of NAT pool usage, use the `show nat pool` command.

```
show nat pool  [cluster]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>cluster</th>
<th>(Optional) When clustering is enabled, shows the current assignment of a PAT address to the owner unit and backup unit.</th>
</tr>
</thead>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A NAT pool is created for each mapped protocol/IP address/port range, where the port ranges are 1-511, 512-1023, and 1024-65535 by default. If you configure the PAT pool to use a flat range of ports, you will see fewer, larger ranges.

Each NAT pool exists for at least 10 minutes after the last usage. The 10 minute hold-down timer is canceled if you clear the translations with `clear xlate`.

**Examples**

The following is sample output for the NAT pools created by a dynamic PAT rule shown by the `show running-config object network` command.

```
> show running-config object network
object network myhost
 host 10.10.10.10
 nat (pppoe2,inside) dynamic 10.76.11.25

> show nat pool
TCP inside, address 10.76.11.25, range 1-511, allocated 0
TCP inside, address 10.76.11.25, range 512-1023, allocated 0
TCP inside, address 10.76.11.25, range 1024-65535, allocated 1
```

The following is sample output from the `show nat pool` command showing use of the PAT pool `flat` option. Without the `include-reserve` keyword, two ranges are shown; the lower range is used when a source port below 1024 is mapped to the same port.

```
> show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
```

The following is sample output from the `show nat pool` command showing use of the PAT pool `flat include-reserve` options.

```
> show nat pool
```
The following is sample output from the `show nat pool` command showing use of the PAT pool
*extended flat include-reserve* options. The important items are the parenthetical addresses. These
are the destination addresses used to extend PAT.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show nat</td>
<td>Displays NAT policy statistics.</td>
</tr>
</tbody>
</table>
show nat proxy-arp

To display the NAT proxy ARP table, use the `show nat proxy-arp` command.

```
show nat proxy-arp [ipv6] [interface name]
```

**Syntax Description**

- `ipv6` (Optional) Shows IPv6 entries in the proxy ARP table.
- `interface name` (Optional) Limits output to the specified source interface.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show nat proxy-arp` command to show runtime representation of the NAT proxy ARP table.

The proxy ARP table shows all NAT commands, even hidden commands. For example, if you configure the management interface to use the data interfaces as a gateway, hidden NAT rules are created for a hidden virtual interface (for example, nlp_int_tap) to enable communications between the management interface and each data interface. These rules are not reflected in the NAT tables in Firepower Device Manager.

**Examples**

The following is sample output from the `show nat proxy-arp` command:

```
> show nat proxy-arp
Nat Proxy-arp Table
id=0x00007f4ce491a010, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
  config:(inside1_8) to (outside) source dynamic any-ipv4 interface
id=0x00007f44ce491d50, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
  config:(inside1_7) to (outside) source dynamic any-ipv4 interface
id=0x00007f4c6138d0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
  config:(inside1_6) to (outside) source dynamic any-ipv4 interface
id=0x00007f4c5a19e70, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
  config:(inside1_5) to (outside) source dynamic any-ipv4 interface
id=0x00007f4c6138d0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
  config:(inside1_4) to (outside) source dynamic any-ipv4 interface
id=0x00007f4c5a19e70, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
  config:(inside1_3) to (outside) source dynamic any-ipv4 interface
id=0x00007f4c5a19e70, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
  config:(inside1_2) to (outside) source dynamic any-ipv4 interface
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear nat counters</td>
<td>Clears NAT policy counters.</td>
</tr>
<tr>
<td>show nat</td>
<td>Displays runtime representation of the NAT policies.</td>
</tr>
</tbody>
</table>
show network

To display the attributes of the management interface, use the `show network` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to view the management interface properties, which you set using the `configure network` commands.

If you configure the management address to use the data interfaces as the gateway, the Gateway is shown as “data-interface.”

### Examples

The following is sample output for the `show network` command.

```
> show network
-------------[ System Information ]-------------
Hostname      : 5516-x-1
Domains       : example.com
DNS Servers   : 10.163.47.11
Management port: 8305
IPv4 Default route
    Gateway : 192.168.0.254
-------------[ br1 ]-------------
State         : Enabled
Channels      : Management & Events
Mode          : Non-Autonegotiation
MDI/MDIX      : Auto/MDIX
MTU           : 1500
-------------[ IPv4 ]-------------
Configuration : Manual
Address       : 192.168.0.166
Netmask       : 255.255.255.0
Broadcast     : 192.168.0.255
-------------[ IPv6 ]-------------
Configuration : Disabled
-------------[ Proxy Information ]-------------
State         : Disabled
Authentication: Disabled
```
show network-dhcp-server

To display the status of the DHCP server on the management interface, use the `show network-dhcp-server` command.

**Command History**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show network-dhcp-server</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to view the status of the optional DHCP server for the management interface. To configure the DHCP server, use the `configure network ipv4 dhcp-server-enable` command.

The output shows whether the DHCP server is enabled or disabled. If enabled, it also shows the address pool.

**Examples**

The following example shows how to configure the DHCP server and show its status.

```
> show network-dhcp-server
DHCP Server Disabled
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure network ipv4 dhcp-server-enable</td>
<td>Configures the DHCP server on the management interface.</td>
</tr>
<tr>
<td>configure network ipv4 dhcp-server-disable</td>
<td>Disables the DHCP server on the management interface.</td>
</tr>
</tbody>
</table>
show network-static-routes

To display static routes configured for the management interface, use the `show network-static-routes` command.

```
show network-static-routes
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Static routes for the management interface are used when you configure multiple management interfaces. These routes do not include the default gateway. If you are using a single management interface, you typically would not have additional static routes.

The routes shown with this command are for the management interface only. They are not used by any data interface. They are not used for through-the-box traffic.

Examples

The following example shows that there are no additional static routes for the management interface. The default gateway is the only route.

```
> show network-static-routes
No static routes currently configured.
```

The following example shows one static route.

```
> show network-static-routes
-----------------------------[ IPv4 Static Routes ]-----------------------------
Interface : br1
Destination : 10.1.1.0
Gateway : 192.168.0.254
Netmask : 255.255.255.0
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure network static-routes</td>
<td>Configure static routes for the management interface.</td>
</tr>
</tbody>
</table>
**show ntp**

To display the current Network Time Protocol (NTP) servers and configuration, use the `show ntp` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays basic information about the NTP servers. If you need more extensive information, use the `system support ntp` command, which includes the output from this command plus the output from the standard NTP command `ntpq`, which is documented with the NTP protocol.

### Examples

The following example shows how to display the NTP configuration.

```
> show ntp
NTP Server   : 209.208.79.69
Status       : Available
Offset       : -1.614 (milliseconds)
Last Update  : 578 (seconds)

NTP Server   : 45.127.112.2  (clocka.ntpjs.org)
Status       : Available
Offset       : -1.355 (milliseconds)
Last Update  : 874 (seconds)

NTP Server   : 198.58.105.63  (ha81.smatwebdesign.com)
Status       : Not Available
Offset       : -4.942 (milliseconds)
Last Update  : 369 (seconds)

NTP Server   : 204.9.54.119  (ntp.your.org)
Status       : Being Used
Offset       : 0.312 (milliseconds)
Last Update  : 962 (seconds)
```

The following example shows how to use the `system support ntp` command to get additional information. Use this command if you need to confirm NTP synchronization.

Look for the section “Results of `ntpq -pn`.” For example, you might see something like the following:

```
> system support ntp
... output redacted ...
Results of 'ntpq -pn'
remote : +216.229.0.50
refid  : 129.7.1.66
st     : 2
t      : u
when   : 704
poll   : 1024
reach  : 377
delay  : 90.455
```
In this example, the + before the NTP server address indicates that it is a potential candidate. An asterisk here, *, indicates the current time source peer.

The NTP deamon (NTPD) uses a sliding window of eight samples from each one of the peers and picks out one sample, then the clock selection determines the true chimers and the false tickers. NTPD then determines the round-trip distance (the offset of a candidate must not be over one-half the round trip delay). If connection delays, packet loss, or server issues cause one or all the candidates to be rejected, you would see long delays in the synchronization. The adjustment also occurs over a very long period of time: the clock offset and oscillator errors must be resolved by the clock discipline algorithm and this can take hours.

If the refid is .LOCL., this indicates the peer is an undisciplined local clock, that is, it is using its local clock only to set the time. Firepower Device Manager always marks the NTP connection yellow (not synchronized) if the selected peer is .LOCL. Normally, NTP does not select a .LOCL. candidate if a better one is available, which is why you should configure at least three servers.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system support ntp</td>
<td>Shows detailed troubleshooting information for NTP.</td>
</tr>
</tbody>
</table>
show object-group

To display object group information and the relevant hit count if the object group is of the network object-group type, use the `show object-group` command.

```
show object-group [network | service | id name]
```

**Syntax Description**

- `id name` (Optional) Identifies an object group by name.
- `network` (Optional) Network type object.
- `service` (Optional) Service-type object.

**Command History**

```
Release    Modification
6.1        This command was introduced.
```

**Examples**

The following is sample output from the `show object-group` command and shows information about the network object group named “Anet”:

```
> show object-group id Anet
Object-group network Anet (hitcnt=10)
   Description OBJ SEARCH ALG APPLIED
   network-object 1.1.1.0 255.255.255.0 (hitcnt=4)
   network-object 2.2.2.0 255.255.255.0 (hitcnt=6)
```

The following is sample output from the `show object-group` command and shows information about a service group:

```
> show object-group service
object-group service B-Serobj
   description its a service group
   service-object tcp eq bgp
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear object-group</td>
<td>Clears the network objects hit count for a given object group.</td>
</tr>
<tr>
<td>show access-list</td>
<td>Shows all access lists, relevant expanded access list entries, and hit counts.</td>
</tr>
</tbody>
</table>
show ospf

To display the general information about the OSPF routing processes, use the `show ospf` command.

```
show ospf [pid [area_id]]
```

### Syntax Description

- **area_id**: (Optional) ID of the area that is associated with the OSPF address range.
- **pid**: (Optional) The ID of the OSPF process.

### Command History

**Release** | **Modification**
--- | ---
6.1 | This command was introduced.

### Examples

The following is sample output from the `show ospf` command, showing how to display general information about a specific OSPF routing process:

```
> show ospf 5
Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0, Checksum Sum 0x 0
Number of opaque AS LSA 0, Checksum Sum 0x 0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

The following is sample output from the `show ospf` command, showing how to display general information about all OSPF routing processes:

```
> show ospf
Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0, Checksum Sum 0x 0
Number of opaque AS LSA 0, Checksum Sum 0x 0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
```
Number of external LSA 0. Checksum Sum 0x 0
Number of opaque AS LSA 0. Checksum Sum 0x 0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
show ospf border-routers

To display the internal OSPF routing table entries to ABRs and ASBRs, use the show ospf border-routers command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show ospf border-routers

OSPF Process 109 internal Routing Table

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

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```
show ospf database

To display the information contained in the OSPF topological database, use the `show ospf database` command.

```
show ospf [pid [area_id]] database [router | network | summary | asbr-summary | external | nssa-external] [lsid] [internal] [self-originate | adv-router addr]
show ospf [pid [area_id]] database database-summary
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>addr</code></td>
<td>(Optional) Router address.</td>
</tr>
<tr>
<td><code>adv-router</code></td>
<td>(Optional) Advertised router.</td>
</tr>
<tr>
<td><code>area_id</code></td>
<td>(Optional) ID of the area that is associated with the OSPF address range.</td>
</tr>
<tr>
<td><code>asbr-summary</code></td>
<td>(Optional) Displays an ASBR list summary.</td>
</tr>
<tr>
<td><code>database</code></td>
<td>Displays the database information.</td>
</tr>
<tr>
<td><code>database-summary</code></td>
<td>(Optional) Displays the complete database summary list.</td>
</tr>
<tr>
<td><code>external</code></td>
<td>(Optional) Displays routes external to a specified autonomous system.</td>
</tr>
<tr>
<td><code>internal</code></td>
<td>(Optional) Routes that are internal to a specified autonomous system.</td>
</tr>
<tr>
<td><code>lsid</code></td>
<td>(Optional) LSA ID.</td>
</tr>
<tr>
<td><code>network</code></td>
<td>(Optional) Displays the OSPF database information about the network.</td>
</tr>
<tr>
<td><code>nssa-external</code></td>
<td>(Optional) Displays the external not-so-stubby-area list.</td>
</tr>
<tr>
<td><code>pid</code></td>
<td>(Optional) ID of the OSPF process.</td>
</tr>
<tr>
<td><code>router</code></td>
<td>(Optional) Displays the router.</td>
</tr>
<tr>
<td><code>self-originate</code></td>
<td>(Optional) Displays the information for the specified autonomous system.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>(Optional) Displays a summary of the list.</td>
</tr>
</tbody>
</table>

**Command History**

```
Release    Modification
6.1         This command was introduced.
```

**Examples**

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

```
> show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

      Router Link States (Area 0)
  Link ID   ADV Router   Age  Seq#  Checksum  Link count
192.168.1.8  192.168.1.8 1381  0x8000010D    0xEF60  2
```

*Cisco Firepower Threat Defense Command Reference*
The following is sample output from the `show ospf database asbr-summary` command:

```plaintext
> show ospf database asbr-summary
OSPF Router with ID (192.168.239.66) (Process ID 300)
Summary ASB Link States (Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links (AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

The following is sample output from the `show ospf database router` command:

```plaintext
> show ospf database router
OSPF Router with id (192.168.239.66) (Process ID 300)
Router Link States (Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 800002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

The following is sample output from the `show ospf database network` command:

```plaintext
> show ospf database network
OSPF Router with id (192.168.239.66) (Process ID 300)
Displaying Net Link States (Area 0.0.0.0)
```
The following is sample output from the `show ospf database summary` command:

```
> show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States (Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links (Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0
```

The following is sample output from the `show ospf database external` command:

```
> show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)
Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```
show ospf events

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

```
show ospf [process_id] events [type]
```

### Syntax Description

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

- **type** *(Optional) A list of the event types you want to see. If you do not specify one or more types, you see all events. You can filter on the following types:*
  - *generic*—Generic events.
  - *interface*—Interface state change events.
  - *lsa*—LSA arrival and LSA generation events.
  - *neighbor*—Neighbor state change events.
  - *reverse*—Show events in reverse order.
  - *rib*—Router Information Base update, delete and redistribution events.
  - *spf*—SPF scheduling and SPF run events.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

```
> show ospf events

OSPF Router with ID (192.168.77.1) (Process ID 5)
1 Apr 27 16:33:23.556: RIB Redist, dest 0.0.0.0, mask 0.0.0.0, Up
2 Apr 27 16:33:23.556: Rescanning RIB: 0x00x0
3 Apr 27 16:33:23.556: Service Redist scan: 0x00x0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ospf</strong></td>
<td>Shows all settings in the OSPF routing process.</td>
</tr>
<tr>
<td><strong>show ospf</strong></td>
<td>Shows the internal OSPF routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).</td>
</tr>
</tbody>
</table>
show ospf flood-list

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

```
show ospf flood-list interface_name
```

**Syntax Description**

| interface_name | The name of the interface for which to display neighbor information. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show ospf flood-list outside

Interface outside, Queue length 20
Link state flooding due in 12 msec

<table>
<thead>
<tr>
<th>Type</th>
<th>LS ID</th>
<th>ADV RTR</th>
<th>Seq NO</th>
<th>Age</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>10.2.195.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0xFB61</td>
</tr>
<tr>
<td>5</td>
<td>10.1.192.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0x2938</td>
</tr>
<tr>
<td>5</td>
<td>10.2.194.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0x757</td>
</tr>
<tr>
<td>5</td>
<td>10.1.193.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0x1E42</td>
</tr>
<tr>
<td>5</td>
<td>10.2.193.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0x124D</td>
</tr>
<tr>
<td>5</td>
<td>10.1.194.0</td>
<td>192.168.0.163</td>
<td>0x80000009</td>
<td>0</td>
<td>0x134C</td>
</tr>
</tbody>
</table>
```
show ospf interface

To display the OSPF-related interface information, use the `show ospf interface` command.

`show ospf interface  [interface_name]`

**Syntax Description**

| interface_name | (Optional) Name of the interface for which to display the OSPF-related information. |

**Command Default**

When you do not specify an interface name, the OSPF information for all interfaces is shown.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show ospf interface outside
out is up, line protocol is up
  Internet Address 10.0.3.4 mask 255.255.255.0, Area 0
  Process ID 2, Router ID 10.0.3.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10 msec, Dead 1, Wait 1, Retransmit 5
  Hello due in 5 msec
  Wait time before Designated router selection 0:00:11
  Index 1/1, flood queue length 0
  Next 0x00000000(0)/0x00000000(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```
show ospf neighbor

To display the OSPF-neighbor information on a per-interface basis, use the show ospf neighbor command.

```
show ospf neighbor [ detail | interface_name [ nbr_router_id ] ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Lists detail information for the specified router.</td>
</tr>
<tr>
<td>interface_name</td>
<td>(Optional) Name of the interface for which to display neighbor information.</td>
</tr>
<tr>
<td>nbr_router_id</td>
<td>(Optional) Router ID of the neighbor router.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the show ospf neighbor command. It shows how to display the OSPF-neighbor information on a per-interface basis.

```
> show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
  In the area 0 via interface outside
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 10.225.200.28 BDR is 10.225.200.30
  Options is 0x42
  Dead timer due in 00:00:36
  Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

The following is sample output from the show ospf neighbor detail command. It shows how to display the detailed information for the specified OSPF-neighbor.

```
> show ospf neighbor detail

Neighbor 25.1.1.60, interface address 15.1.1.60
  In the area 0 via interface inside
  Neighbor priority is 1, State is FULL, 46 state changes
  DR is 15.1.1.62 BDR is 15.1.1.60
  Options is 0x12 in Hello (E-bit, L-bit)
  Options is 0x52 in DBD (E-bit, L-bit, O-bit)
  LLS Options is 0x1 (LR), last OOB-Resync 00:03:07 ago
  Dead timer due in 00:00:24
  Neighbor is up for 01:42:15
  Index 5/5, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 0, maximum is 0
  Last retransmission scan time is 0 msec, maximum is 0 msec
```
show ospf nsf

To display the OSPFv2 related NSF information, use the `show ospf nsf` command.

show ospf nsf

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show ospf nsf` command:

```
> show ospf nsf
Routing Process "ospf 10"
Non-Stop Forwarding enabled
  Clustering is not configured in spanned etherchannel mode
IETF NSF helper support enabled
Cisco NSF helper support enabled
  OSPF restart state is
    Handle 1, Router ID 25.1.1.60, checkpoint Router ID 0.0.0.0
    Config wait timer interval 10, timer not running
    Dbase wait timer interval 120, timer not running
```
show ospf request-list

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

```
show ospf request-list  nbr_router_id interface_name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface_name</td>
<td>Name of the interface for which to display neighbor information. Displays the list of all LSAs that are requested by the router from this interface.</td>
</tr>
<tr>
<td>nbr_router_id</td>
<td>Router ID of the neighbor router. Displays the list of all LSAs that are requested by the router from this neighbor.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
> show ospf request-list 192.168.1.12 inside

    OSPF Router with ID (192.168.1.11) (Process ID 1)

    Neighbor 192.168.1.12, interface inside address 172.16.1.12

    Type  LS ID          ADV RTR     Seq NO       Age  Checksum
      1  192.168.1.12    192.168.1.12  0x8000020D  8   0x6572
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ospf retransmission-list</td>
<td>Displays a list of all LSAs waiting to be resent.</td>
</tr>
</tbody>
</table>
show ospf retransmission-list

To display a list of all LSAs waiting to be resent for a specific neighbor and interface, use the `show ospf retransmission-list` command.

`show ospf retransmission-list  nbr_router_id interface_name`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface_name</code></td>
<td>Name of the interface for which to display neighbor information.</td>
</tr>
<tr>
<td><code>nbr_router_id</code></td>
<td>Router ID of the neighbor router.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show ospf retransmission-list` command for the 192.168.1.11 neighbor router on the outside interface.

```plaintext
> show ospf retransmission-list 192.168.1.11 outside

OSPF Router with ID (192.168.1.12) (Process ID 1)
Neighbor 192.168.1.11, interface outside address 172.16.1.11

Link state retransmission due in 3764 msec, Queue length 2
  Type  LS ID       ADV RTR     Seq NO  Age  Checksum
     1  192.168.1.12  192.168.1.12 0x80000210 0  0xB196
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ospf request-list</code></td>
<td>Displays a list of all LSAs that are requested by a router.</td>
</tr>
</tbody>
</table>
show ospf rib

To display the OSPF Router Information Base (RIB), use the show ospf rib command

```
show ospf [process_id [area_id]] rib [network_prefix [network_mask]] | detail | redistribution [network_prefix [network_mask]] | detail ]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process_id</td>
</tr>
<tr>
<td>area_id</td>
</tr>
<tr>
<td>network_prefix [network_mask]</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>detail</td>
</tr>
<tr>
<td>redistribution</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
</tr>
<tr>
<td>Modification</td>
</tr>
<tr>
<td>6.1</td>
</tr>
<tr>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show ospf statistics**

To display various OSPF statistics, such as the number of times SPF was executed, the reasons, and the duration, use the `show ospf statistics` command.

```
show ospf [process_id] statistics [detail]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detail</code></td>
<td>(Optional) Specifies detailed SPF information, including the trigger points.</td>
</tr>
<tr>
<td><code>process_id</code></td>
<td>(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show ospf statistics` command:

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

SPF 1 executed 04:36:56 ago, SPF type Full
SPF calculation time (in msec):
   SPT   Prefix  D-Int  Sum  D-Sum  Ext  D-Ext  Total
   0      0        0      0      0      0      0      0
RIB manipulation time (in msec):
   RIB Update  RIB Delete
   0            0
LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X:7:0
Change record R L
LSAs changed 2
Changed LSAs. Recorded is Advertising Router, LSID and LS type:
   49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
SPF calculation time (in msec):
   SPT   Prefix  D-Int  Sum  D-Sum  Ext  D-Ext  Total
   0      0        0      0      0      0      0      0
RIB manipulation time (in msec):
   RIB Update  RIB Delete
   0            0
LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X:7:0
Change record R N L
LSAs changed 5
Changed LSAs. Recorded is Advertising Router, LSID and LS type:
   50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R) 50.100.168.192/2(N)
```
show ospf summary-address

To display a list of all summary address redistribution information that is configured under an OSPF process, use the `show ospf summary-address` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following shows sample output from the `show ospf summary-address` command. It shows how to display a list of all summary address redistribution information before a summary address has been configured for an OSPF process with the ID of 5.

```plaintext
> show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```
show ospf traffic

To display a list of different types of packets that have been processed (sent or received) by a particular OSPF instance, use the `show ospf traffic` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

With this command, you can get a snapshot of the different types of OSPF packets that are being processed without enabling debugging. If there are two OSPF instances configured, the `show ospf traffic` command displays the statistics for both instances with the process ID of each instance. You can also display the statistics for a single instance by using the `show ospf process_id traffic` command.

### Examples

The following shows sample output from the `show ospf traffic` command.

```plaintext
> show ospf traffic

OSPF statistics (Process ID 70):

    Rcvd: 244 total, 0 checksum errors
    234 hello, 4 database desc, 1 link state req
    3 link state updates, 2 link state acks
    Sent: 485 total
    472 hello, 7 database desc, 1 link state req
    3 link state updates, 2 link state acks
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ospf virtual-links</td>
<td>Displays the parameters and the current state of OSPF virtual links.</td>
</tr>
</tbody>
</table>
show ospf virtual-links

To display the parameters and the current state of OSPF virtual links, use the `show ospf virtual-links` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

```
> show ospf virtual-links
Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```
show ospf virtual-links
show p - show r

- show pager, on page 775
- show packet debugs, on page 776
- show parser dump, on page 778
- show password encryption, on page 779
- show pclu, on page 780
- show perfmon, on page 781
- show perfstats, on page 782
- show pim bsr-router, on page 783
- show pim df, on page 784
- show pim group-map, on page 785
- show pim interface, on page 786
- show pim join-prune statistic, on page 787
- show pim neighbor, on page 788
- show pim range-list, on page 789
- show pim topology, on page 790
- show pim traffic, on page 792
- show pim tunnel, on page 793
- show policy-list, on page 794
- show policy-route, on page 795
- show port-channel, on page 796
- show port-channel load-balance, on page 800
- show power inline, on page 802
- show prefix-list, on page 803
- show priority-queue, on page 805
- show processes, on page 807
- show process-tree, on page 810
- show ptp, on page 811
- show quota, on page 813
- show resource types, on page 814
- show resource usage, on page 815
- show rip database, on page 817
- show rollback-status, on page 818
- show route, on page 819
• show route-map, on page 822
• show rule hits, on page 823
• show running-config, on page 825
show pager

To display the current page length for the CLI session, that is, the number of lines shown before the output pauses with a -- More -- indication, use the `show pager` command.

```plaintext
> show pager
no pager
```

You cannot set the page length for the Firepower Threat Defense CLI.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show pager` command. Because you cannot set the page length in the Firepower Threat Defense CLI, the output indicates that there is no pager.
show packet debugs

To retrieve and view the stored debug logs from the database use `show packet debugs` command.

```
show packet debugs  [match [protocol]   [   source-ip]  [source-port]  [dest-ip]  [dest-port]
[module module-id]  [packet-id packet-id]   [severity 0-7]  [time-start time]  [time-end time]
```

**Syntax Description**

- **match**: Matches one or more of the following options entered for filtering connection: source IP, destination IP, source port, destination port or protocol.
- **protocol**: Name of the protocol.
- **source-ip**: IP address of the source.
- **source-port**: Port number of the source.
- **dest-ip**: IP address of the destination.
- **dest-port**: Port number of the destination.
- **module module-id**: The module name to filter the debug logs.
- **packet-id packet-id**: The unique packet id to filter the debug logs.
- **severity 0-7**: One of the following severity levels:
  - 0 (emergencies)—System is unusable
  - 1 (alert)—Immediate action is needed
  - 2 (critical)—Critical conditions
  - 3 (error)—Error conditions
  - 4 (warning)—Warning conditions
  - 5 (notice)—Normal but significant conditions
  - 6 (informational)—Informational messages only
  - 7 (debug)—Debugging messages only
- **time-start time**: Returns all logs after the specified start time.
- **time-end time**: Returns all logs before the specified time.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use `show packet debugs` command to retrieve and view the stored debug logs from the database.
All keywords within [ ] are optional. If a particular keyword is not entered, that keyword would be considered as any. All the debugs are displayed in the ascending order of timestamp.

**Examples**
The following example enables TCP debugging, then shows debugging status.

> show packet debugs

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug</td>
<td>Enables debugging.</td>
</tr>
</tbody>
</table>
show parser dump

The `show parser dump` command is for internal or Cisco Technical Support use.
show password encryption

To show the password encryption configuration settings, use the show password encryption command.

show password encryption

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Firepower Threat Defense does not allow you to configure master password encryption, so this command should always show that password encryption is Disabled and that the master key hash is not set.

If the key has been saved, “saved” appears next to the key hash. If there is no key or it has been removed from the running configuration, “Not set” appears instead of the hash value.

Examples

The following is sample output from the show password encryption command:

> show password encryption
Password Encryption: Disabled
Master key hash: Not set(saved)
show pclu

The show pclu command is for internal or Cisco Technical Support use.
show perfmon

To display information about the performance of the device, use the *show perfmon* command.

```
show perfmon  [detail]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Shows additional statistics. These statistics match those gathered by the Global and Per-protocol connection objects of the Cisco Unified Firewall MIB.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The *perfmon* command shows performance statistics continuously at defined intervals. The *show perfmon* command allows you to display the information immediately.

**Examples**

The following is sample output for the *show perfmon detail* command:

```
> show perfmon detail
PERFMON STATS:  Current  Average
Xlates       0/s   0/s
Connections  0/s   0/s
TCP Conns    0/s   0/s
UDP Conns    0/s   0/s
URL Access   0/s   0/s
URL Server Req 0/s  0/s
TCP Fixup    0/s   0/s
HTTP Fixup   0/s   0/s
FTP Fixup    0/s   0/s
AAA Authen   0/s   0/s
AAA Author   0/s   0/s
AAA Account  0/s   0/s
TCP Intercept 0/s  0/s
SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>perfmon</td>
<td>Displays detailed performance monitoring information at defined intervals.</td>
</tr>
</tbody>
</table>
show perfstats

To display performance statistics for the device, use the `show perfstats` command.

**show perfstats**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show perfstats` command shows performance information for the Detection Engines. The command shows you a list of available engines, you pick the one whose statistics you want to view. You are then presented with a number of profiles; select the one whose content you want to view.

The files are meaningful for systems managed remotely by Firepower Management Center. These files typically have no content for systems managed with the local manager, Firepower Device Manager.

Use Ctrl+C to stop the display if you decide you do not want to see the complete file. The file contents can be long.

**Examples**

```
> show perfstats
Available DEs:
  1 - Primary Detection Engine (703006f4-8ff6-11e6-bb6e-8f2d5febf243)
  0 - Cancel and return to CLI
Select a DE to profile: 1
Available now files:
  1 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febfb243/2016-10-13
  2 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febfb243/2016-10-16
  3 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febfb243/2016-10-11
  4 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febfb243/2016-10-15
  5 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febfb243/2016-10-14
  6 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febfb243/2016-10-12
  7 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febfb243/instance-1/now
  0 - Cancel and return to DE selection
Select a now file: 7
Mon Oct 17 00:05:00 2016
  Pkts Recv: 162
  Pkts Drop: 0
  Block Verdicts: 0
  Mbits/Sec: 0.001
  Drop Rate: 0%
  Alerts/Sec: 0
  Total Alerts/Sec: 0
(...remaining content truncated...)```
show pim bsr-router

To display the bootstrap router (BSR) information, use the show pim bsr-router command.

```
show pim bsr-router
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the show pim bsr-router command:

```
> show pim bsr-router
PIMv2 Bootstrap information
This system is a candidate BSR
  Candidate BSR interface GigabitEthernet0/0 is down - BSR messages not originated
  Candidate RP: 4.4.4.1(GigabitEthernet0/0), GigabitEthernet0/0 is down - not advertised
```
show pim df

To display the bidirectional DF “winner” for a rendezvous point (RP) or interface, use the `show pim df` command.

```
show pim df  [winner]  [rp_address  | interface_name]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rp_address</code></td>
<td>Can be either one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Name of the RP, as defined in the Domain Name System (DNS) hosts table.</td>
</tr>
<tr>
<td></td>
<td>• IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.</td>
</tr>
<tr>
<td><code>interface_name</code></td>
<td>The physical or logical interface name.</td>
</tr>
<tr>
<td><code>winner</code></td>
<td>(Optional) Displays the DF election winner per interface per RP.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command also displays the winner metric towards the RP.

**Examples**

The following is sample output from the `show pim df` command:

```
> show pim df
RP           Interface  DF Winner  Metrics
172.16.1.3   Loopback3  172.17.3.2  [110/2]
172.16.1.3   Loopback2  172.17.2.2  [110/2]
172.16.1.3   Loopback1  172.17.1.2  [110/2]
172.16.1.3   inside     10.10.2.3  [0/0]
172.16.1.3   inside     10.10.1.2  [110/2]
```
show pim group-map

To display group-to-protocol mapping table, use the show pim group-map command.

```
show pim group-map [info-source | rp-timers] [group]
```

### Syntax Description

- **group** *(Optional) Can be one of the following:
  - Name of the multicast group, as defined in the DNS hosts table.
  - IPv4 or IPV6 address of the multicast group.

- **info-source** *(Optional) Displays the group range information source.

- **rp-timers** *(Optional) Displays uptime and expiry timers of group-to-RP mapping.

### Command Default

Displays group-to-protocol mappings for all groups.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays all group protocol address mappings for the RP. Mappings are learned on the device from different clients.

The PIM implementation on the device has various special entries in the mapping table. Auto-rp group ranges are specifically denied from sparse-mode group range. SSM group range also does not fall under sparse-mode. Link Local multicast groups (224.0.0.0–224.0.0.225, as defined by 224.0.0.0/24) are also denied from the sparse-mode group range. The last entry shows all remaining groups in Sparse-Mode with a given RP.

### Examples

The following is sample output form the show pim group-map command:

```
> show pim group-map
Group Range  Proto  Client Groups  RP address  Info
224.0.1.39/32*  DM  static 1  0.0.0.0
224.0.1.40/32*  DM  static 1  0.0.0.0
224.0.0.0/24*  NO  static 0  0.0.0.0
232.0.0.0/8*  SSM  config 0  0.0.0.0
224.0.0.0/4*  SM  autorp 1  10.10.2.2  RPF: POS01/0/3,10.10.3.2
```

In lines 1 and 2, Auto-RP group ranges are specifically denied from the sparse mode group range.

In line 3, link-local multicast groups (224.0.0.0 to 224.0.0.255 as defined by 224.0.0.0/24) are also denied from the sparse mode group range.

In line 4, the PIM Source Specific Multicast (PIM-SSM) group range is mapped to 232.0.0.0/8.

The last entry shows that all the remaining groups are in sparse mode mapped to RP 10.10.3.2.
show pim interface

To display interface-specific information for PIM, use the `show pim interface` command.

```
show pim interface [interface_name | state-off | state-on]
```

**Syntax Description**

- `interface_name` (Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
- `state-off` (Optional) Displays interfaces with PIM disabled.
- `state-on` (Optional) Displays interfaces with PIM enabled.

**Command Default**

If you do not specify an interface, PIM information for all interfaces is shown.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The Firepower Threat Defense device is itself a PIM neighbor. Therefore, the neighbor count column in the output of this command shows one more than the actual number of neighbors.

**Examples**

The following example displays PIM information for the inside interface:

```
> show pim interface inside
Address  Interface  Ver/ Nbr  Query  DR  DR
        Mode    Intvl  Prior
172.16.1.4 inside v2/S  2  100 ms  1  172.16.1.4
```
show pim join-prune statistic

To display PIM join/prune aggregation statistics, use the `show pim join-prune statistic` command.

```
show pim join-prune statistic [interface_name]
```

**Syntax Description**

- `interface_name` (Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

**Command Default**

If an interface is not specified, this command shows the join/prune statistics for all interfaces.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Clear the PIM join/prune statistics with the `clear pim counters` command.

**Examples**

The following is sample output from the `show pim join-prune statistic` command:

```
> show pim join-prune statistic
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface Transmitted Received
inside 0 / 0 / 0 0 / 0 / 0
GigabitEthernet1 0 / 0 / 0 0 / 0 / 0
    Ethernet0 0 / 0 / 0 0 / 0 / 0
    Ethernet2 0 / 0 / 0 0 / 0 / 0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear pim counters</td>
<td>Clears the PIM traffic counters.</td>
</tr>
</tbody>
</table>
**show pim neighbor**

To display entries in the PIM neighbor table, use the `show pim neighbor` command.

```
show pim neighbor [count | detail] [interface]
```

**Syntax Description**

- **interface** (Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
- **count** (Optional) Displays the total number of PIM neighbors and the number of PIM neighbors on each interface.
- **detail** (Optional) Displays additional address of the neighbor learned through the upstream-detection hello option.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used to determine the PIM neighbors known to this router through PIM hello messages. Also, this command indicates that an interface is a designated router (DR) and when the neighbor is capable of bidirectional operation.

The Firepower Threat Defense device is itself a PIM neighbor. Therefore, the Firepower Threat Defense interface is shown in the output of this command. The IP address of the Firepower Threat Defense device is indicated by an asterisk next to the address.

**Examples**

The following is sample output from the `show pim neighbor` command:

```
> show pim neighbor inside
Neighbor Address  Interface  Uptime   Expires  DR  pri Bidir
10.10.1.1        inside     03:40:36 00:01:41  1   B
10.10.1.2*        inside     03:41:28 00:01:32  (DR) B
```
show pim range-list

To display range-list information for PIM, use the `show pim range-list` command.

```
show pim range-list [config] [rp_address]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Displays PIM CLI range list information.</td>
</tr>
<tr>
<td>rp_address</td>
<td>Can be either one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Name of the rendezvous point (RP), as defined in the Domain Name System</td>
</tr>
<tr>
<td></td>
<td>(DNS) hosts table.</td>
</tr>
<tr>
<td></td>
<td>• IP address of the RP. This is a multicast IP address in four-part</td>
</tr>
<tr>
<td></td>
<td>dotted-decimal notation.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used to determine the multicast forwarding mode to group mapping. The output also indicates the rendezvous point (RP) address for the range, if applicable.

**Examples**

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

```
> show pim range-list
  config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
  config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
  config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
  config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim group-map</td>
<td>Displays group-to-PIM mode mapping and active RP information.</td>
</tr>
</tbody>
</table>
show pim topology

To display PIM topology table information, use the `show pim topology` command.

```
show pim topology [reserved | route-count [detail] | group [source]]
```

### Syntax Description

- **reserved**: Display PIM topology table information for reserved groups.
- **route-count**: Shows the number of routes in the PIM topology table.
- **detail**: (Optional) Displays more detailed count information on a per-group basis.
- **group**: (Optional) Can be one of the following:
  - Name of the multicast group, as defined in the DNS hosts table.
  - IPv4 or IPV6 address of the multicast group.
- **source**: (Optional) Can be one of the following:
  - Name of the multicast source, as defined in the DNS hosts table.
  - IPv4 or IPV6 address of the multicast source.

### Command Default

Topology information for all groups and sources is shown.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the MRIB, which is an intermediary for communication between multicast routing protocols, such as PIM, local membership protocols, such as Internet Group Management Protocol (IGMP), and the multicast forwarding engine of the system.

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

### Note

For forwarding information, use the `show mfib route` command.

### Examples

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

```
> show pim topology
```
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
outside 15:57:24 off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
outside 15:57:20 fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
outside 15:57:16 fwd LI LH

The following is sample output from the `show pim topology reserved` command:

> show pim topology reserved
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
RR - Register Received, SR - Sending Registers, E - MSDP External,
DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
II - Internal Interest, ID - Internal Disinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
outside 00:02:26 off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
inside 00:00:48 off II

The following is sample output from the `show pim topology route-count` command:

> show pim topology route-count
PIM Topology Table Summary
No. of group ranges = 5
No. of (*/G) routes = 0
No. of (S,G) routes = 0
No. of (S,G)RPT routes = 0

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mrib route</td>
<td>Displays the MRIB table.</td>
</tr>
</tbody>
</table>
**show pim traffic**

To display PIM traffic counters, use the `show pim traffic` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Clear the PIM traffic counters with the `clear pim counters` command.

### Examples

The following is sample output from the `show pim traffic` command:

```
> show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

<table>
<thead>
<tr>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid PIM Packets</td>
<td>0</td>
</tr>
<tr>
<td>Hello</td>
<td>0</td>
</tr>
<tr>
<td>Join-Prune</td>
<td>0</td>
</tr>
<tr>
<td>Register</td>
<td>0</td>
</tr>
<tr>
<td>Register Stop</td>
<td>0</td>
</tr>
<tr>
<td>Assert</td>
<td>0</td>
</tr>
<tr>
<td>Bidir DF Election</td>
<td>0</td>
</tr>
</tbody>
</table>

Errors:
Malformed Packets | 0
Bad Checksums     | 0
Send Errors        | 0
Packet Sent on Loopback Errors | 0
Packets Received on PIM-disabled Interface | 0
Packets Received with Unknown PIM Version | 0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear pim counters</td>
<td>Clears the PIM traffic counters.</td>
</tr>
</tbody>
</table>
show pim tunnel

To display information about the PIM tunnel interfaces, use the `show pim tunnel` command.

```
show pim tunnel  [interface_name]
```

**Syntax Description**

- `interface_name` (Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

**Command Default**

If an interface is not specified, this command shows the PIM tunnel information for all interfaces.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

PIM register packets are sent through the virtual encapsulation tunnel interface from the source first hop DR router to the rendezvous point (RP). On the RP, a virtual decapsulation tunnel is used to represent the receiving interface of the PIM register packets. This command displays tunnel information for both types of interfaces. Register tunnels are the encapsulated (in PIM register messages) multicast packets from a source that is sent to the RP for distribution through the shared tree. Registering applies only to SM, not SSM and bidirectional PIM.

**Examples**

The following is sample output from the `show pim tunnel` command:

```
> show pim tunnel
Interface  RP Address Source Address
Encapstunne 10.1.1.1 10.1.1.1
Decapstunne 10.1.1.1 -
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show pim topology</code></td>
<td>Displays the PIM topology table.</td>
</tr>
</tbody>
</table>
show policy-list

To display information about a configured policy list and policy list entries, use the `show policy-list` command.

```
show policy-list [policy_list_name]
```

**Syntax Description**

- `policy_list_name` (Optional) Display information about the specified policy list.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Policy lists are used in BGP routing as matching criteria for route maps.

**Examples**

The following is sample output from the `show policy-list` command:

```
> show policy-list

policy-list policy_list_2 permit
  Match clauses:
    ip address prefix-lists: prefix_1

policy-list policy_list_1 permit
  Match clauses:
    ip address (access-lists): test
    interface inside
```
show policy-route

To show policy-based routing configurations, use the **show policy-route** command.

**show policy-route**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

```plaintext
> show policy-route
Interface Route map
GigabitEthernet0/0   equal-access
```
show port-channel

To display EtherChannel information in a detailed and one-line summary form or to display the port and port-channel information, use the **show port-channel** command.

`show port-channel [channel_group_number] [brief | detail | port | protocol | summary]`

**Syntax Description**

- **brief**: (Default) Shows a brief display.
- **channel_group_number**: (Optional) Specifies the EtherChannel channel group number, between 1 and 48, and only shows information about this channel group.
- **detail**: (Optional) Shows a detailed display.
- **port**: (Optional) Shows information for each interface.
- **protocol**: (Optional) Shows the EtherChannel protocol, such as LACP if enabled.
- **summary**: (Optional) Shows a summary of port-channels.

**Command Default**

The default is **brief**.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 6.1     | This command was introduced.

**Examples**

The following is sample output from the **show port-channel** command:

```plaintext
> show port-channel
Channel-group listing:
-----------------------
Group: 1
--------
Ports: 3  Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
```

The following is sample output from the **show port-channel summary** command:

```plaintext
> show port-channel summary
Number of channel-groups in use: 1
Group  Port-channel  Protocol  Ports
-------------------------------------
1      Po1            LACP     Gi3/1    Gi3/2    Gi3/3
```
The following is sample output from the `show port-channel detail` command:

```markdown
> show port-channel detail
    Channel-group listing:
    -----------------------

Group: 1
--------
Ports: 3  Maxports = 16
Port-channels: 1  Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip

    Ports in the group:
    -------------------

Port: Gi3/1
--------
Port state  = bndl
Channel group = 1  Mode = LACP/ active
Port-channel = Po1
Flags:  S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs.
        A - Device is in active mode.  P - Device is in passive mode.

Local information:
<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/1</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x302</td>
<td>0x3d</td>
</tr>
</tbody>
</table>

Partner's information:
<table>
<thead>
<tr>
<th>Partner</th>
<th>Partner</th>
<th>LACP Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Flags</td>
<td>State</td>
<td>LACP Partner</td>
<td>Admin Key</td>
<td>Oper Key</td>
<td>Port Number</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-------</td>
<td>---------------</td>
<td>-----------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>Gi3/1</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x0</td>
<td>0x1</td>
<td>0x306</td>
</tr>
</tbody>
</table>

Port: Gi3/2
--------
Port state  = bndl
Channel group = 1  Mode = LACP/ active
Port-channel = Po1
Flags:  S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs.
        A - Device is in active mode.  P - Device is in passive mode.

Local information:
<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/2</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x303</td>
<td>0x3d</td>
</tr>
</tbody>
</table>

Partner's information:
<table>
<thead>
<tr>
<th>Partner</th>
<th>Partner</th>
<th>LACP Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Flags</td>
<td>State</td>
<td>LACP Partner</td>
<td>Admin Key</td>
<td>Oper Key</td>
<td>Port Number</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-------</td>
<td>---------------</td>
<td>-----------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>Gi3/2</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x0</td>
<td>0x1</td>
<td>0x303</td>
</tr>
</tbody>
</table>

Port: Gi3/3
--------
Port state  = bndl
Channel group = 1  Mode = LACP/ active
```
Port-channel = Po1

Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs.
A - Device is in active mode.  P - Device is in passive mode.

Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/3</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x304</td>
<td>0x3d</td>
<td></td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>Partner</th>
<th>Partner</th>
<th>LACP Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Flags</td>
<td>State</td>
<td>Port Priority</td>
<td>Admin Key</td>
<td>Oper Key</td>
<td>Port Number</td>
<td>Port State</td>
</tr>
<tr>
<td>Gi3/3</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x0</td>
<td>0x1</td>
<td>0x302</td>
<td>0x3d</td>
</tr>
</tbody>
</table>

The following is sample output from the `show port-channel port` command:

```plaintext
> show port-channel port
Channel-group listing:

Group: 1

Port: Gi3/1

- Port state = bndl
- Channel group = 1
- Mode = LACP/ active
- Port-channel = Po1

Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs.
A - Device is in active mode.  P - Device is in passive mode.

Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/1</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x302</td>
<td>0x3d</td>
<td></td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>Partner</th>
<th>Partner</th>
<th>LACP Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Flags</td>
<td>State</td>
<td>Port Priority</td>
<td>Admin Key</td>
<td>Oper Key</td>
<td>Port Number</td>
<td>Port State</td>
</tr>
<tr>
<td>Gi3/1</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x0</td>
<td>0x1</td>
<td>0x306</td>
<td>0x3d</td>
</tr>
</tbody>
</table>

Port: Gi3/2

- Port state = bndl
- Channel group = 1
- Mode = LACP/ active
- Port-channel = Po1

Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs.
A - Device is in active mode.  P - Device is in passive mode.

Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/2</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x303</td>
<td>0x3d</td>
<td></td>
</tr>
</tbody>
</table>
```
The following is sample output from the `show port-channel protocol` command:

```markdown
> show port-channel protocol
Channel-group listing:
-----------
Group: 1
-----------
Protocol: LACP
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show lacp</code></td>
<td>Displays LACP information such as traffic statistics, system identifier, and neighbor details.</td>
</tr>
<tr>
<td><code>show port-channel load-balance</code></td>
<td>Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.</td>
</tr>
</tbody>
</table>
show port-channel load-balance

For EtherChannels, to display the current port-channel load-balance algorithm, and optionally to view the member interface selected for a given set of parameters, use the `show port-channel load-balance` command.

```
show port-channel channel_group_number load-balance [hash-result { (ip | ipv6 | mac | l4port | mixed) parameters | vlan-only number }]
```

**Syntax Description**

- `channel_group_number`: Specifies the EtherChannel channel group number, between 1 and 48.
- `hash-result`: (Optional) Shows the member interface chosen after hashing values you enter for the current load-balancing algorithm.
- `ip`: (Optional) Specifies IPv4 packet parameters.
- `ipv6`: (Optional) Specifies IPv6 packet parameters.
- `l4port`: (Optional) Specifies port packet parameters.
- `mac`: (Optional) Specifies MAC address packet parameters.
- `mixed`: (Optional) Specifies a combination of IP or IPv6 parameters, along with ports and/or the VLAN ID.
- `parameters`: (Optional) Packet parameters, depending on the type. For example, for `ip`, you can specify the source IP address, the destination IP address, and/or the VLAN ID.
- `vlan-only number`: (Optional) Specifies the VLAN ID for a packet, from 0-4095.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, the device balances the packet load on interfaces according to the source and destination IP address (src-dst-ip) of the packet.

This command lets you view the current load-balancing algorithm, but, with the `hash-result` keyword, also lets you test which member interface will be chosen for a packet with given parameters. This command only tests against the current load-balancing algorithm. For example, if the algorithm is src-dst-ip, then enter the IPv4 or IPv6 source and destination IP addresses. If you enter other arguments not used by the current algorithm, they are ignored, and the unentered values actually used by the algorithm default to 0. For example, if the algorithm is vlan-src-ip, then enter:

```
show port-channel 1 load-balance hash-result ip source 10.1.1.1 vlan 5
```

If you enter the following, then the vlan-src-ip algorithm assumes a source IP address of 0.0.0.0 and VLAN 0, and ignores the values you enter:
show port-channel 1 load-balance hash-result l4port source 90 destination 100

Examples

The following is sample output from the `show port-channel 1 load-balance` command:

```
> show port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
  src-dst-ip
EtherChannel Load-Balancing Addresses Used Per-Protocol:
  Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination IP address
  IPv6: Source XOR Destination IP address
```

The following is sample output from the `show port-channel 1 load-balance hash-result` command, where the entered parameters match the current algorithm (src-dst-ip):

```
> show port-channel 1 load-balance hash-result ip source 10.1.1.1 destination 10.5.5.5
Would select GigabitEthernet2/1 based on algorithm src-dst-ip
```

The following is sample output from the `show port-channel 1 load-balance hash-result` command, where the entered parameters do not match the current algorithm (src-dst-ip), and the hash uses 0 values:

```
> show port-channel 1 load-balance hash-result l4port source 5
Would select GigabitEthernet3/2 of Port-channel1 based on algorithm src-dst-ip
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lacp</td>
<td>Displays LACP information such as traffic statistics, system identifier and neighbor details.</td>
</tr>
<tr>
<td>show port-channel</td>
<td>Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.</td>
</tr>
</tbody>
</table>
show power inline

For models with PoE interfaces, use the `show power inline` command to show power status of the interfaces.

**Note**

Supported for the Firepower 1010 only.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use PoE interfaces to connect devices that require power, such as an IP phone or a wireless access point. For the Firepower 1010, Ethernet 1/7 and 1/8 support PoE+.

**Examples**

The following is sample output from the `show power inline` command for the Firepower 1010:

```
> show power inline
  Interface  Power  Class  Current (mA)  Voltage (V)
  ----------  ------  ------  ----------------  --------
  Ethernet1/1  n/a    n/a    n/a  n/a
  Ethernet1/2  n/a    n/a    n/a  n/a
  Ethernet1/3  n/a    n/a    n/a  n/a
  Ethernet1/4  n/a    n/a    n/a  n/a
  Ethernet1/5  n/a    n/a    n/a  n/a
  Ethernet1/6  n/a    n/a    n/a  n/a
  Ethernet1/7  On     4      121.00   53.00
  Ethernet1/8  On     4      88.00    53.00
```

The following table shows each field description:

**Table 47: show power inline Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Shows all interfaces on the FTD, including ones that do not have PoE available.</td>
</tr>
<tr>
<td>Power</td>
<td>Shows whether the power is On or Off. If a device does not need power, if there is no device on that interface, or if the interface is shut down the value is Off. If the interface does not support PoE, then the value is n/a.</td>
</tr>
<tr>
<td>Class</td>
<td>Shows the PoE class of the connected device.</td>
</tr>
<tr>
<td>Current (mA)</td>
<td>Shows the current being used.</td>
</tr>
<tr>
<td>Voltage (V)</td>
<td>Shows the voltage being used.</td>
</tr>
</tbody>
</table>
show prefix-list

To list prefix lists that are configured to match IPv4 traffic, use the `show prefix-list` command.

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

**Syntax Description**
- **detail**: Show details about prefix lists.
- **summary**: Show a summary of prefix lists.
- **prefix_list_name**: Name of a prefix list.
- **seq sequence_number**: (Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix list.
- **network/length [longer | first-match]**: (Optional) Displays all entries in the specified prefix list that use this network address and netmask length (in bits). The length of the network mask can be from 0 to 32.

You can optionally include one of the following keywords:

- **longer**: displays all entries of the specified prefix list that match or are more specific than the given network/length.
- **first-match**: displays the first entry of the specified prefix list that matches the given network/length.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show prefix-list` command with a prefix-list named “test.”

```
> show prefix-list detail test
prefix-list test:   Description: test-list
   count: 1, range entries: 0, sequences: 1 - 1, refcount: 3
      seq 1 permit 2.0.0.0/8 (hit count: 0, refcount: 1)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear prefix-list</td>
<td>Reset the hit count on an IP prefix list.</td>
</tr>
<tr>
<td>show bgp prefix-list</td>
<td>Displays information about a prefix list or prefix list entries in the context of Border Gateway Protocol.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><code>show ipv6 prefix-list</code></td>
<td>Displays information about IPv6 prefix lists.</td>
</tr>
</tbody>
</table>
show priority-queue

To display the priority-queue configuration or statistics for an interface, use the `show priority-queue` command.

`show priority-queue {config | statistics} [interface_name]`

**Syntax Description**

- **config** 
  Show the queue and TX-ring limits for the interface priority queues.

- **interface_name** 
  (Optional) Specifies the name of the interface for which you want to show the configuration or the best-effort and low-latency queue statistical details.

- **statistics** 
  Show the best-effort and low-latency queue statistical details.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows statistics for the interface named test. In the output, BE indicates the best-effort queue, and LLQ represents the low-latency queue:

```
> show priority-queue statistics test
Priority-Queue Statistics interface test
Queue Type  = BE
Packets Dropped  = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length  = 0
Max Q Length      = 0
Queue Type  = LLQ
Packets Dropped  = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length  = 0
Max Q Length      = 0
```

The following example shows the configuration of the priority queues on all configured interfaces.

```
> show priority-queue config
Priority-Queue Config interface inside
  current  default  range
queue-limit  0      2048   0 - 2048
tx-ring-limit 4294967295 511 3 - 511
Priority-Queue Config interface test
  current  default  range
queue-limit  0      2048   0 - 2048
tx-ring-limit 4294967295 511 3 - 511
```
### show priority-queue

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear priority-queue statistics</td>
<td>Resets priority queue statistics to zero.</td>
</tr>
</tbody>
</table>

#### Priority-Queue Config

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Current</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>outside</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tx-ring-limit</td>
<td></td>
<td>4294967295</td>
<td>511</td>
<td>3 - 511</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Current</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgmember1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tx-ring-limit</td>
<td></td>
<td>4294967295</td>
<td>511</td>
<td>3 - 511</td>
</tr>
</tbody>
</table>
show processes

To display a list of the processes that are running on the device, use the `show processes` command.

```
show processes [ cpu-hog | cpu-usage [non-zero] [sorted] | internals | memory | system ]
```

### Syntax Description

- **cpu-hog**: Shows number and detail of processes that are hogging the CPU (that is, using the CPU for more than 100 milliseconds).
- **cpu-usage**: Shows percentage of CPU used by each process for the last 5 seconds, 1 minute and 5 minutes.
- **internals**: Shows internal details of each process.
- **memory**: Shows memory allocation for each process.
- **non-zero**: (Optional) Shows processes with non-zero CPU usage.
- **sorted**: (Optional) Shows sorted CPU usage for processes.
- **system**: (Optional) Shows information about the processes currently running on the system.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Processes are lightweight threads that require only a few instructions. The `show processes` commands display a list of the processes that are running on the device, as follows:

<table>
<thead>
<tr>
<th>Command</th>
<th>Data Displayed</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show processes</td>
<td>PC</td>
<td>Program counter.</td>
</tr>
<tr>
<td>show processes</td>
<td>SP</td>
<td>Stack pointer.</td>
</tr>
<tr>
<td>show processes</td>
<td>STATE</td>
<td>Address of thread queue.</td>
</tr>
<tr>
<td>show processes</td>
<td>Runtime</td>
<td>Number of milliseconds that the thread has been running based on CPU clock cycles. The accuracy is within one millisecond for complete and accurate accounting of process CPU usage based on CPU clock cycles (&lt;10ns resolution) instead of clock ticks (10ms resolution).</td>
</tr>
<tr>
<td>show processes cpu-usage</td>
<td>SBASE</td>
<td>Stack base address.</td>
</tr>
<tr>
<td>show processes</td>
<td>Stack</td>
<td>Current number of bytes in use and the total size of the stack.</td>
</tr>
<tr>
<td>show processes</td>
<td>Process</td>
<td>Function of the thread.</td>
</tr>
<tr>
<td>show processes cpu-usage</td>
<td>MAXHOG</td>
<td>Maximum CPU hog runtime in milliseconds.</td>
</tr>
<tr>
<td>Command</td>
<td>Data Displayed</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>show processes cpu-usage</td>
<td>NUMHOG</td>
<td>Number of CPU hog runs.</td>
</tr>
<tr>
<td>show processes cpu-usage</td>
<td>LASTHOG</td>
<td>Last CPU hog runtime in milliseconds.</td>
</tr>
<tr>
<td>show processes cpu-usage</td>
<td>PC</td>
<td>Instruction pointer of the CPU hogging process.</td>
</tr>
<tr>
<td>show processes cpu-usage</td>
<td>Traceback</td>
<td>Stack trace of the CPU hogging process. The traceback can have up to 14 addresses.</td>
</tr>
<tr>
<td>show processes internals</td>
<td>Invoked Calls</td>
<td>Number of times the scheduler ran the process.</td>
</tr>
<tr>
<td>show processes internals</td>
<td>Giveups</td>
<td>Number of times the process yielded the CPU back to the scheduler.</td>
</tr>
</tbody>
</table>

Use the `show processes cpu-usage` command to narrow down a particular process on the device that might be using the CPU. You can use the `sorted` and `non-zero` commands to further customize the output of the `show processes cpu-usage` command.

With the scheduler and total summary lines, you can run two consecutive `show processes` commands and compare the output to determine:

- Consumption of 100% of the CPU.
- Percentage of CPU used by each thread, determined by comparing the runtime delta of a thread to the total runtime delta.

The device runs as a single process with many different threads of execution. The output of this command actually shows memory allocations and free memory on a per-thread basis. Because these threads work in cooperation on data flows and other operations pertinent to operation of the device, one thread may allocate a block of memory while a different thread may free it. The last row of output contains the total counts over all threads. Only this row may be used to track potential memory leaks by monitoring the difference between allocations and free memory.

**Examples**

The following example shows how to display a list of processes that are running. Command output wraps.

```
> show processes
PC SP STATE Runtime SBASE
Stack Process TID
Mwe 0x00007f9ae994881e 0x00007f9acbf4d6e18 0x00007f9b027e1340 0 0x00007f9acb9cf030
32000/32768 zone_background_idb 140
Mwe 0x00007f9ae91d64ae 0x00007f9ae765919d8 0x00007f9b027e1340 0 0x00007f9ae7652030
27568/32768 WebVPN KCD Process 14
Msi 0x00007f9aca38e04 0x00007f9acba86e48 0x00007f9b027e1340 2917 0x00007f9acba7f030
29944/32768 vpnlb_timer_thread 131

The following example shows how to list system processes.
```

```
> show processes system
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND

Cisco Firepower Threat Defense Command Reference
The following example shows how to display the percentage of CPU used by each process:

```bash
> show processes cpu-usage non-zero
```

<table>
<thead>
<tr>
<th>PC</th>
<th>Thread</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00007f9ae8abcc76</td>
<td>0x00007f9ad04cf7a0</td>
<td>0.2%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>Environment Monitor</td>
</tr>
</tbody>
</table>

The following examples show how to display the number and detail of processes that are hogging the CPU:

```bash
> show processes cpu-hog
```

Process: cli_xml_server, NUMHOG: 12, MAXHOG: 30, LASTHOG: 2
LASTHOG At: 17:37:08 UTC Oct 28 2016
PC: 0x00007f9ae9b11539 (suspend)
Call stack: 0x00007f9ae9b11539 0x00007f9ae9caf084 0x00007f9ae9caf9d0 0x00007f9ae8736425 0x00007f9ae9b13346 0x00007f9ae9b15ab4 0x00007f9ae8730ead 0x00007f9ae87663ec 0x00007f9ae6ecde0 0x00007f9ac4a46120 0x31223d646920696c

The following example shows how to display the memory allocation for each process:

```bash
> show processes memory
```

<table>
<thead>
<tr>
<th>Allocs</th>
<th>Allocated (bytes)</th>
<th>Frees</th>
<th>Freed (bytes)</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td><em>System Main</em></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>QoS Support Module</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>SSL</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>vpnfol_thread_sync Monitor</td>
</tr>
<tr>
<td>22</td>
<td>8636</td>
<td>78</td>
<td>3728</td>
<td>DHCP Network Scope</td>
</tr>
<tr>
<td>7</td>
<td>40459</td>
<td>0</td>
<td>0</td>
<td>Integrity FW Task</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>uauth_urlb clean</td>
</tr>
<tr>
<td>2</td>
<td>64</td>
<td>0</td>
<td>0</td>
<td>arp_timer</td>
</tr>
<tr>
<td>8450</td>
<td>233220</td>
<td>0</td>
<td>0</td>
<td>HDD Health Monitor</td>
</tr>
<tr>
<td>14638</td>
<td>1659384</td>
<td>14509</td>
<td>1570750</td>
<td>PTHREAD-23518</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>6</td>
<td>1926</td>
<td>DHCP Client</td>
</tr>
</tbody>
</table>

The following example shows how to display the internal details of each process:

```bash
> show processes internals
```

<table>
<thead>
<tr>
<th>Invoked</th>
<th>Giveups</th>
<th>Max_Runtime</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0.002</td>
<td>zone_background_idb</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0.163</td>
<td>WebVPN KCD Process</td>
</tr>
<tr>
<td>507512</td>
<td>0</td>
<td>0.060</td>
<td>vpnlb_timer_thread</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0.057</td>
<td>vpnlb_thread</td>
</tr>
<tr>
<td>2029820</td>
<td>0</td>
<td>0.130</td>
<td>vpnfol_thread_unsent</td>
</tr>
<tr>
<td>507455</td>
<td>0</td>
<td>0.137</td>
<td>vpnfol_thread_timer</td>
</tr>
</tbody>
</table>

(...output truncated...)
show process-tree

To display the system processes in a tree relationship, use the **show process-tree** command.

**show process-tree**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output for this command is mainly of interest to Cisco Technical Support.

**Examples**

The following is an example of showing the process tree.

```
> show process-tree
init(1)-+-acpid(23138)
   |+-agetty(23726)
   |+-crond(23141)
   |+-dbus-daemon(23119)
   |+-login(23727)-+-clish(6394)
   |                |-{nscl}(14445)-+-{nscl}(14448)
   |                |                   |-{nscl}(14449)
   |                |                   |-{nscl}(14450)
   |                |                   |-{nscl}(14451)
   |                |                   |-{nscl}(14452)
   |                |                   |`-{nscl}(14453)
   (...remaining output truncated...)```
show ptp

To display Precision Time Protocol (PTP) statistics and clock information, use the `show ptp` command.

```
show ptp { clock | port [interface_name] }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock</td>
<td>Displays PTP clock properties.</td>
</tr>
<tr>
<td>port [interface_name]</td>
<td>Displays PTP port information for the interfaces. You can optionally specify an interface name to see information about that interface only.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Example

The following example shows that PTP is not configured. PTP packets can pass through the device, but the device does not use the PTP clocks.

```
> show ptp clock
No clock information is available in PTP forwarding mode.
> show ptp port
No clock information is available in PTP forwarding mode.
```

The following example shows PTP clock properties:

```
> show ptp clock
PTP CLOCK INFO
PTP Device Type: Transparent Clock
Operation mode: One Step
Clock Identity: 0:8:2F:FF:FE:E8:43:81
Clock Domain: 0
Number of PTP ports: 4
```

The following example shows PTP port information for all PTP-enabled interfaces:

```
> show ptp port
PTP PORT DATASET: GigabitEthernet1/1
Port identity: port number: 1
PTP version: 2
Port state: Enabled

PTP PORT DATASET: GigabitEthernet1/2
Port identity: port number: 2
PTP version: 2
Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/3
Port identity: port number: 3
PTP version: 2
```
Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
Port identity: port number: 4
PTP version: 2
Port state: Enabled
show quota

To show quota statistics for the current session, use the `show quota` command.

```
show quota [management-session]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>management-session</td>
<td>Shows statistics for the current management session.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You cannot configure management session quotas on Firepower Threat Defense. This command should always show no limits.

**Examples**

The following example shows quota statistics.

```
> show quota
quota management-session limit 0
quota management-session warning level 0
quota management-session level 0
quota management-session high water 0
quota management-session errors 0
quota management-session warnings 0
```
show resource types

To view the resource types for which the device tracks usage, use the `show resource types` command.

**show resource types**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following sample display shows the resource types:

```
> show resource types
Rate limited resource types:
  Conns       Connections/sec
  Inspects    Inspects/sec
  Syslogs     Syslogs/sec

Absolute limit types:
  Conns       Connections
  Hosts       Hosts
  IPSec       IPSec Mgmt Tunnels
  Mac-addresses  MAC Address table entries
  ASDM       ASDM Connections
  SSH Client SSH Client Sessions
  SSH Server SSH Server Sessions
  Storage     Storage Limit Size of context directory in MB
  Telnet     Telnet Sessions
  Xlates     XLATE Objects
  Routes     Routing Table Entries
  All        All Resources
  Other VPN Sessions Other VPN Sessions
  Other VPN Burst Allowable burst for Other VPN Sessions
  AnyConnect AnyConnect Premium licensed sessions
  AnyConnect Burst Allowable burst for AnyConnect Premium licensed sessions
  IKEv1 in-negotiation Allowable in negotiation IKEv1 SAs
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear resource usage</td>
<td>Clears the resource usage statistics</td>
</tr>
<tr>
<td>show resource usage</td>
<td>Shows the resource usage of the device.</td>
</tr>
</tbody>
</table>
show resource usage

To view the resource usage of the device, use the show resource usage command.

```
show resource usage [all | detail] [resource { [rate] resource_name | all } ] [counter counter_name [count_threshold] ]
```

### Syntax Description
- `all` All types.
- `count_threshold` Sets the number above which resources are shown. The default is 1. If the usage of the resource is below the number you set, then the resource is not shown. If you specify `all` for the counter name, then the count threshold applies to the current usage. To show all resources, set the count threshold to 0.
- `counter counter_name` Shows counts for the following counter types:
  - `current`—Shows the active concurrent instances or the current rate of the resource.
  - `peak`—Shows the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either using the clear resource usage command or because the device rebooted.
  - `denied`—Shows the number of instances that were denied because they exceeded the resource limit shown in the Limit column.
  - `all`—(Default) Shows all statistics.
- `detail` Shows the resource usage of all resources, including those you cannot manage. For example, you can view the number of TCP intercepts.
- `resource {[rate] resource_name | all}` Shows the usage of a specific resource. Specify `all` for all resources. Specify rate to show the rate of usage of a resource. Resources that are measured by rate include `conns`, `inspects`, and `syslogs`. You must specify the `rate` keyword with these resource types. The `conns` resource is also measured as concurrent connections; only use the `rate` keyword to view the connections per second. See the Usage Guidelines section for a list of resource names.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When you use the `resource` keyword, resources include the following types:
- `asdm`—The feature related to this keyword is not supported by Firepower Threat Defense.
- `conns`—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts.
- `hosts`—Hosts that can connect through the Firepower Threat Defense device.
- `ipsec`—IPSec management tunnels
• **mac-addresses**—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.

• **rate**—Rate-measured resources. Specify **conns**, **inspects**, or **syslogs**.

• **routes**—Routing Table entries.

• **ssh**—SSH sessions.

• **storage**—Storage Limit Size, in MB.

• **telnet**—Telnet sessions.

• **vpn**—VPN resources.

• **vpn anyconnect**—AnyConnect Premium license limit.

• **vpn ikev1 in-negotiation**—Number of IKEv1 sessions which can be in negotiation.

• **VPN Other**—Site-to-site VPN sessions.

• **VPN Burst Other**—Site-to-site VPN burst sessions.

• **xlates**—NAT translations.

**Examples**

The following is sample output from the `show resource usage` command, which shows the resource usage for all resources. The device is in single context mode, so the context is shown as System.

```
> show resource usage
Resource            Current  Peak  Limit  Denied Context
Syslogs [rate]      0       144  N/A    0 System
Conns               0       5    100000 0 System
Xlates              0       5  N/A    0 System
Hosts               0       8  N/A    0 System
Conns [rate]        0       1  N/A    0 System
Inspects [rate]     0       3  N/A    0 System
Mac-addresses       0       4  16384  0 System
Routes              9       9  unlimited 0 System
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear resource usage</td>
<td>Clears the resource usage statistics</td>
</tr>
<tr>
<td>show resource types</td>
<td>Shows a list of resource types.</td>
</tr>
</tbody>
</table>
show rip database

To display the information that is stored in the RIP topological database, use the `show rip database` command.

```
show rip database [ip_addr [mask]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip_addr</code></td>
<td>(Optional) Limits the display routes for the specified network address.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>(Optional) Specifies the network mask for the optional network address.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The RIP database contains all of the routes learned through RIP. Routes that appear in this database may not necessarily appear in the routing table.

**Examples**

The following is sample output from the `show rip database` command:

```
> show rip database

10.0.0.0/8    auto-summary
10.11.0.0/24   directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16   int-summary
10.11.10.0/24  directly connected, GigabitEthernet0/3
192.168.1.1/24
   [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

The following is sample output from the `show rip database` command with a network address and mask:

```
> show rip database 172.19.86.0 255.255.255.0

172.19.86.0/24
   [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
   [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```
show rollback-status

To show the status of the latest rollback job (if any) sent from Firepower Management Center, use the `show rollback-status` command.

```
> show rollback-status
  Status    : None
  Start Time : N/A
  End Time   : N/A
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If Firepower Management Center needs to roll back configuration changes during a deployment job, it sends a request to the device and then the management connection from Firepower Management Center to the device is reset. You can use this command to see the status of the rollback job.

The rollback job relates to the commands configured in the running configuration file only; it does not roll back the Snort configuration.

If the device is running in high availability mode, use this command on the active unit only. In a cluster, use the command on the master unit only.

The information includes the following:

- **Status**—The status of the most recent rollback job.
  - None—No rollback job has been ever requested.
  - In Progress—The system has received the rollback request, and the rollback job is in progress.
  - Succeeded—The rollback has completed successfully.
  - Reverted—Rollback to the configuration sent from Firepower Device Manager failed. The system reverts to the last saved configuration.
  - Failed—Rollback completed with error.

- **Start Time/End Time**—The starting and ending times for the job. N/A means there was no job; for end time, N/A can also mean that the job is still in progress.

**Examples**

The following example shows the normal situation, where no rollback job has ever been requested.

```
> show rollback-status
  Status    : None
  Start Time : N/A
  End Time   : N/A
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Shows the configuration that is defined in the running configuration file.</td>
</tr>
</tbody>
</table>
show route

To display the routing table for the data interfaces, use the `show route` command.

```
show route [management-only] [cluster] [failover] [ip_address [mask] [longer-prefixes]] [bgp [as_number]] [connected] [eigrp [process_id]] [isis] [ospf [process_id]] [rip] [static] [summary] [zone]
```

### Syntax Description

- **bgp as_number**  
  (Optional) Displays the routing information base (RIB) epoch number (sequence number), the current timer value, and the network descriptor block epoch number (sequence number) for the BGP route. The AS number limits the display to route entries that use the specified AS number.

- **cluster**  
  (Optional) Displays the routing information base (RIB) epoch number (sequence number), the current timer value, and the network descriptor block epoch number (sequence number).

- **connected**  
  (Optional) Displays connected routes.

- **eigrp process_id**  
  (Optional) Displays EIGRP routes. Firepower Threat Defense does not support EIGRP, however.

- **failover**  
  (Optional) Displays the current sequence number of the routing table and routing entries after failover has occurred, and a standby unit becomes the active unit.

- **interface_name**  
  (Optional) Displays route entries that use the specified interface.

- **ip_address mask**  
  (Optional) Displays routes to the specified destination.

- **isis**  
  (Optional) Displays IS-IS routes.

- **longer-prefixes**  
  (Optional) Displays routes that match the specified ip_address/mask pair only.

- **management-only**  
  (Optional) Displays routes in the IPv4 management routing table.

- **ospf process_id**  
  (Optional) Displays OSPF routes.

- **rip**  
  (Optional) Displays RIP routes.

- **static**  
  (Optional) Displays static routes.

- **summary**  
  (Optional) Displays the current state of the routing table.

- **zone**  
  (Optional) Displays the routes for zone interfaces.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `show route` command provides output similar to the `show ipv6 route` command, except that the information is IPv4-specific. The routes shown are for the data interfaces only, not for the virtual management interface.
To see the default gateway for the management interface, use the `show network` command. To see routes on the management interface, use the `show network-static-routes` command.

The clustering and failover keywords do not appear unless these features are configured on the Firepower Threat Defense device.

The `show route` command lists the “best” routes for new connections. When you send a permitted TCP SYN to the backup interface, the Firepower Threat Defense device can only respond using the same interface. If there is no default route in the RIB on that interface, the device drops the packet because of no adjacency. Everything that is configured as shown in the `show running-config route` command is maintained in certain data structures in the system.

You can check the backend interface-specific routing table with the `show asp table routing` command. This design is similar to OSPF or EIGRP, in which the protocol-specific route database is not the same as the global routing table, which only displays the “best” routes. This behavior is by design.

**Examples**

The following is sample output from the `show route` command:

```plaintext
> show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C 10.86.194.0 255.255.255.0 is directly connected, outside
C 10.40.10.0 255.255.255.0 is directly connected, inside
C 192.168.2.0 255.255.255.0 is directly connected, faillink
C 192.168.3.0 255.255.255.0 is directly connected, statelink

The following is sample output of the `show route failover` command, which shows the synchronization of OSPF and EIGRP routes to the standby unit after failover:

```plaintext
> show route failover

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0
Routing table sequence number 1
Reconvergence timer 00.20 (Running)
S  10.10.10.0 255.0.0.0 [1/0] via 10.10.10.1, mgmt, seq 1
```
The following is sample output from the `show route cluster` command:

```
> show route cluster
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, s - IS-IS summary, U - per-user static route, o - ODR
      P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set
Routing table seq num 2
Reconvergence timer expires in 52 secs

C  70.0.0.0 255.255.255.0 is directly connected, cluster, seq 1
C  172.23.0.0 255.255.0.0 is directly connected, tftp, seq 1
C  200.165.200.0 255.255.255.0 is directly connected, outside, seq 1
C  198.51.100.0 255.255.255.0 is directly connected, inside, seq 1
O  198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 2
D  209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 2
```

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

```
> show route summary
IP routing table maximum-paths is 3
Routing table seq num 2
Reconvergence timer expires in 52 secs

Route Source     Networks Subnets Replicates Overhead Memory (bytes)
connected         0       2       0      176      576
static            1       0       0       88      288
bgp 2             0       0       0       0       0
  External: 0 Internal: 0 Local: 0
internal          1
Total             2       2       0      264     1272
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 route</code></td>
<td>Shows the IPv6 routing table.</td>
</tr>
</tbody>
</table>
show route-map

To show route map information, use the `show route-map` command.

```
show route-map [ all | dynamic [ application [ application ] | detail | route_map ] | route_map ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Show information about both static and dynamic route maps.</td>
</tr>
<tr>
<td><code>dynamic</code></td>
<td>Show only information about dynamic route maps.</td>
</tr>
<tr>
<td><code>application</code></td>
<td>Application that created the route map.</td>
</tr>
<tr>
<td><code>route_map</code></td>
<td>Name of the route map.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

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

```bash
> show route-map dynamic
route-map MIP-10/24/06-05:23:46.091-1- MPATH_1, permit, sequence 0, identifier 54943520
  Match clauses:
    ip address (access-lists): VOICE
  Set clauses:
    interface Tunnel0
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```
show rule hits

To display rule hit information for all evaluated rules of access control policies and prefilter policies, use the `show rule hits` command.

```
show rule hits [ id  |  raw  |  gt #hit-count  |  lt #hit-count  |  range #hit-count1 #hit-count2 ]
```

**Syntax Description**

- `id` (Optional) The ID of a rule. Including this argument limits the displayed information to the specified rule.
- `raw` (Optional) Displays the rule hit information in .csv format.
- `gt #hit-count` (Optional) Displays all the rules that have a hit count greater than `#hit-count`.
- `lt #hit-count` (Optional) Displays all the rules that have a hit count lesser than `#hit-count`.
- `range #hit-count1 #hit-count2` (Optional) Displays all the rules that have a hit count in-between `#hit-count1` and `#hit-count2`.

**Command Default**

If you do not specify a rule ID, the rule hit information for all the rules are shown.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The rule hit information covers only the access control rules and prefilter rules.

**Examples**

The following example displays rule hit information:

```plaintext
> show rule hits
RuleID   Hit Count  First Hit Time(UTC)   Last Hit Time(UTC)
-----------------  -------------- -------------------  -------------------
268436981     2  22:02:00 Jan 25 2019  22:02:02 Jan 25 2019
```
## show rule hits

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear rule hits</td>
<td>Clears the rule hit information for all evaluated rules of access control policies and prefilter policies and resets them to zero.</td>
</tr>
<tr>
<td>show cluster rule hits</td>
<td>Display rule hit information for all evaluated rules of access control policies and prefilter policies from all nodes of a cluster in an aggregated format.</td>
</tr>
<tr>
<td>cluster exec show rule hits</td>
<td>Display rule hit information for all evaluated rules of access control policies and prefilter policies from each node of a cluster in a segregated format.</td>
</tr>
<tr>
<td>cluster exec clear rule hits</td>
<td>Clears rule hit information for all evaluated rules of access control policies and prefilter policies and reset them to zero, from all nodes in a cluster.</td>
</tr>
</tbody>
</table>
show running-config

To display the configuration that is currently running on the device, use the show running-config command.

```
show running-config [all] [command]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Displays the entire operating configuration, including defaults.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>command</td>
<td>Displays the configuration associated with a specific command. For available commands, see the CLI help using show running-config ?.</td>
</tr>
</tbody>
</table>

**Note** Firepower Threat Defense does not directly support every command listed in the CLI help. There might not be any configuration for a given option. Some options can be configured only using a FlexConfig from Firepower Management Center.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The show running-config command displays the active configuration in memory (including saved configuration changes) on the device. You cannot directly configure these commands. Instead, they are configured by the manager controlling the device, for example, Firepower Management Center or Firepower Device Manager.

However, this is a partial configuration. It shows what can be configured using ASA Software configuration commands only, although some commands might be specific to Firepower Threat Defense. These commands are ported to Firepower Threat Defense. Thus, you should use the information in the running configuration as a troubleshooting aid only. Use the device manager as the main means to analyze the device configuration.

**Examples**

The following is sample output from the show running-config command:

```
> show running-config
: Saved
:
: Serial Number: XXXXXXXXXXX
: Hardware: ASA5512, 4096 MB RAM, CPU Clarkdale 2793 MHz, 1 CPU (2 cores)
: NGFW Version 6.1.0
! hostname firepower
enable password $sha512$5000$Col980QPR9Vvq/VYoAKGJw==$ZvzuZDNpcvEP/DGbBqytA== pbkdf2 strong-encryption-disable
names
!
interface GigabitEthernet0/0
 nameif outside
cs manual
propagate sgt preserve-untag
```
policy static sgt disabled trusted
security-level 0
ip address 192.168.10.1 255.255.255.0
ipv6 enable

interface GigabitEthernet0/1
shutdown
nameif inside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.1 255.255.255.0
ipv6 enable

interface GigabitEthernet0/2
shutdown
nameif dmz
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.2.1 255.255.255.0
ipv6 enable

interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/5
shutdown
no nameif
no security-level
no ip address

interface Management0/0
management-only
no nameif
no security-level
no ip address

ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: Initial AC Policy - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
access-list CSM_IPSEC_ACL_1 extended permit ip any any6 any6
show running-config

tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
tcp-options md5 clear
urgent-flag allow
!
no pager
logging enable
logging buffer informational
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
access-group CSM_FW_ACL_global
as-path access-list 2 deny 100$
as-path access-list 2 permit 200$
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 actcp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mcp 0:05:00 mcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
aaa proxy-limit disable
no snmp-server location
no snmp-server contact
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
no sysopt connection permit-vpn
crypto ipsec ikev1 transform-set CSM_TS_1 esp-des esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map CSM_outside_map 1 match address CSM_IPSEC_ACL_1
crypto map CSM_outside_map 1 set peer 10.10.10.10
crypto map CSM_outside_map 1 set ikev1 transform-set CSM_TS_1
crypto map CSM_outside_map 1 set reverse-route
crypto map CSM_outside_map interface outside
crypto ca trustpool policy
crypto ikev1 enable outside
crypto ikev1 policy 160
authentication pre-share
cipher des
des hash sha
group 5
tunnel-group 10.10.10.10 lifetime 86400
telnet timeout 5
telnet timeout 0
dynamic-access-policy-record DfltAccessPolicy
tunnel-group 10.10.10.10 type ipsec-l2l
tunnel-group 10.10.10.10 ipsec-attributes
ikev1 pre-shared-key *****
!
class-map inspection_default
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
!
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
router-alert action allow
!
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect smtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
!
set connection advanced-options UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:167911f11cbf1140edeffcb0f9b17f01
; end
>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-control-config</td>
<td>Shows summary information about the access control policy.</td>
</tr>
</tbody>
</table>
show s - sz

• show sctp, on page 831
• show serial-number, on page 833
• show service-policy, on page 834
• show shun, on page 840
• show sip, on page 841
• show skinny, on page 842
• show sla monitor, on page 843
• show snmp-server, on page 845
• show snort counters, on page 847
• show snort instances, on page 850
• show snort preprocessor-memory-usage, on page 851
• show snort statistics, on page 853
• show snort tls-offload, on page 856
• show software authenticity, on page 858
• show ssh-access-list, on page 861
• show ssl, on page 862
• show ssl-policy-config, on page 865
• show ssl-protocol, on page 867
• show startup-config, on page 868
• show summary, on page 869
• show sunrpc-server active, on page 870
• show switch mac-address-table, on page 871
• show switch vlan, on page 873
• show tcpstat, on page 875
• show tech-support, on page 878
• show threat-detection memory, on page 879
• show threat-detection rate, on page 881
• show threat-detection scanning-threat, on page 883
• show threat-detection shun, on page 884
• show threat-detection statistics, on page 885
• show time, on page 894
• show time-range, on page 895
• show tls-proxy, on page 896
• show track, on page 898
• show traffic, on page 899
• show user, on page 900
• show version, on page 902
• show vlan, on page 904
• show vm, on page 905
• show vpdn, on page 906
• show vpn load-balancing, on page 908
• show vpn-sessiondb, on page 909
• show vpn-sessiondb ratio, on page 921
• show vpn-sessiondb summary, on page 923
• show wccp, on page 925
• show webvpn, on page 927
• show xlate, on page 929
• show zone, on page 931
• shun, on page 933
• shutdown, on page 935
• system access-control clear-rule-counts, on page 936
• system generate-troubleshoot, on page 937
• system lockdown-sensor, on page 939
• system support commands, on page 940
• system support ssl-client-hello- commands, on page 941
• system support diagnostic-cli, on page 942
• system support ssl-hw- commands, on page 944
• system support view-files, on page 947
show sctp

To display current Stream Control Transmission Protocol (SCTP) cookies and associations, use the show sctp command.

show sctp  [detail]

Syntax Description

detail  Displays detailed information about SCTP associations.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The show sctp command displays information about SCTP cookies and associations.

If you enable SCTP inspection using a FlexConfig from Firepower Management Center, this command can show the SCTP information.

Examples

The following is sample output from the show sctp command:

> show sctp
AssocID: 2279da7a
Local: 192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40174 (ESTABLISHED)
AssocID: 4924f520
Local: 192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40200 (ESTABLISHED)

The following is sample output from the show sctp detail command:

> show sctp detail
AssocID: 8b7e3fffb
Local: 192.168.100.56/3868 (ESTABLISHED)
  Receiver Window: 48000
  Cumulative TSN: 5cb6cd9b
  Next TSN: 5cb6cd9c
  Earliest Outstanding TSN: 5cb6cd9c
  Out-of-Order Packet Count: 0
Remote: 192.168.200.78/3868 (ESTABLISHED)
  Receiver Window: 114688
  Cumulative TSN: 5cb6cd98
  Next TSN: 0
  Earliest Outstanding TSN: 5cb6cd9c
  Out-of-Order Packet Count: 0
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show local-host</td>
<td>Shows information on hosts making connections through the device, per interface.</td>
</tr>
<tr>
<td>show service-policy inspect sctp</td>
<td>Shows SCTP inspection statistics.</td>
</tr>
<tr>
<td>show traffic</td>
<td>Shows connection and inspection statistics per interface</td>
</tr>
</tbody>
</table>
show serial-number

To display the chassis serial number, use the `show serial-number` command. This command is not available on virtual devices.

```
show serial-number
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show serial-number` command to view the device’s serial number. This information is also shown in `show version system` and `show running-config` output.

**Examples**

The following example shows how to display the serial number. The number in this example has been changed to be invalid.

```
> show serial-number
XXX175078X5
```
show service-policy

To display the service policy statistics, use the show service-policy command.

show service-policy [global | interface intf] [cluster flow-mobility | inspect inspection [arguments] | police | priority | set connection [details] | sfr | shape | user-statistics]

show service-policy [global | interface intf] [flow protocol {host src_host | src_ip src_mask}] [eq src_port | {host dest_host | dest_ip dest_mask} [eq dest_port] [icmp_number | icmp_control_message] ]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster flow-mobility</td>
<td>(Optional.) Shows status information on flow mobility in Firepower Threat Defense clusters.</td>
</tr>
<tr>
<td>dest_ip dest_mask</td>
<td>For the flow keyword, the destination IP address and netmask of the traffic flow.</td>
</tr>
<tr>
<td>details</td>
<td>(Optional) For the set connection keyword, displays per-client connection information, if a per-client connection limit is enabled.</td>
</tr>
<tr>
<td>eq dest_port</td>
<td>(Optional) For the flow keyword, equals the destination port for the flow.</td>
</tr>
<tr>
<td>eq src_port</td>
<td>(Optional) For the flow keyword, equals the source port for the flow.</td>
</tr>
<tr>
<td>flow protocol</td>
<td>(Optional) Shows policies that match a particular flow identified by the 5-tuple (protocol, source IP address, source port, destination IP address, destination port). You can use this command to check that your service policy configuration will provide the services you want for specific connections.</td>
</tr>
<tr>
<td>global</td>
<td>(Optional) Limits output to the global policy.</td>
</tr>
<tr>
<td>host dest_host</td>
<td>For the flow keyword, the host destination IP address of the traffic flow.</td>
</tr>
<tr>
<td>host src_host</td>
<td>For the flow keyword, the host source IP address of the traffic flow.</td>
</tr>
<tr>
<td>icmp_control_message</td>
<td>(Optional) For the flow keyword when you specify ICMP as the protocol, specifies an ICMP control message of the traffic flow.</td>
</tr>
<tr>
<td>icmp_number</td>
<td>(Optional) For the flow keyword when you specify ICMP as the protocol, specifies the ICMP protocol number of the traffic flow.</td>
</tr>
<tr>
<td>inspect inspection [arguments]</td>
<td>(Optional) Shows detailed information about policies that include an inspect command. Not all inspect commands are supported for detailed output. To see all inspections, use the show service-policy inspect ? command. The arguments available for each inspection vary; see the CLI help for more information.</td>
</tr>
<tr>
<td>interface intf</td>
<td>(Optional) Displays policies applied to the interface specified by the intf argument, where intf is the interface name.</td>
</tr>
<tr>
<td>police</td>
<td>(Optional) Shows detailed information about policies that include the police command.</td>
</tr>
<tr>
<td>priority</td>
<td>(Optional) Shows detailed information about policies that include the priority command.</td>
</tr>
</tbody>
</table>
show service-policy

<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you do not specify any arguments, this command shows all global and interface policies.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The number of embryonic connections displayed in the `show service-policy` command output indicates the current number of embryonic connections to an interface for traffic matching that defined for a traffic class. The “embryonic-conn-max” field shows the maximum embryonic limit configured for the traffic class. If the current embryonic connections displayed equals or exceeds the maximum, TCP intercept is applied to new TCP connections that match the traffic.

When you make service policy changes to the configuration, all new connections use the new service policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. `show` command output will not include data about the old connections. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy. See the `clear conn` or `clear local-host` commands.

You cannot directly configure service policies using Firepower Management Center or Firepower Device Manager. Some changes are made indirectly when you edit various connection settings or configure QoS policies. You can also adjust which default inspections are enabled using the `configure inspection` command. If you use FlexConfig in Firepower Management Center to configure service policies, this command shows statistics related to your configuration.

**Note**

For an `inspect icmp` and `inspect icmp error` policies, the packet counts only include the echo request and reply packets.

**Examples**

The following is sample output for the `show service-policy` command.

```
> show service-policy
Global policy:
  Service-policy: global_policy
```
show service-policy

Global policy:
Service-policy: global_policy
Class-map: inspection_default

Set connection advanced-options: UM_STATIC_TCP_MAP
Retransmission drops: 0 TCP checksum drops : 0
Exceeded MSS drops : 0 SYN with data drops: 0
Invalid ACK drops : 0 SYN-ACK with data drops: 0
Out-of-order (OoO) packets : 0 OoO no buffer drops: 0
OoO buffer timeout drops : 0 SEQ past window drops: 0
Reserved bit cleared: 0 Reserved bit drops : 0
IP TTL modified : 0 Urgent flag cleared: 0
Window varied resets: 0
TCP-options:
  Selective ACK cleared: 0 Timestamp cleared : 0
  Window scale cleared : 0
  Other options cleared: 0
  Other options drops: 0

For devices that have multiple CPU cores, there is a counter for lock failure. The locking mechanism is used to protect shared data structures and variables, because they can be used by multiple cores. When the core fails to acquire a lock, it tries to get the lock again. The lock fail counter increments for each failed attempt.

> show service-policy

Global policy:
Service-policy: global_policy
Class-map: inspection_default

...
Inspect: esmtp _default_esmtp_map, packet 96716502, lock fail 7, drop 25, reset-drop 0
Inspect: sqlnet, packet 2526511491, lock fail 21, drop 2362, reset-drop 0

The following command shows the statistics for GTP inspection. The output is explained in the table that follows the example.

> `show service-policy inspect gtp statistics`

GPRS GTP Statistics:

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version_not_support</td>
<td>Displays packets with an unsupported GTP version field.</td>
</tr>
<tr>
<td>msg_too_short</td>
<td>Displays packets less than 8 bytes in length.</td>
</tr>
<tr>
<td>unknown_msg</td>
<td>Displays unknown type messages.</td>
</tr>
<tr>
<td>unexpected_sig_msg</td>
<td>Displays unexpected signaling messages.</td>
</tr>
<tr>
<td>unexpected_data_msg</td>
<td>Displays unexpected data messages.</td>
</tr>
<tr>
<td>mandatory_ie_missing</td>
<td>Displays messages missing a mandatory Information Element (IE).</td>
</tr>
<tr>
<td>mandatory_ie_incorrect</td>
<td>Displays messages with an incorrectly formatted mandatory Information Element (IE).</td>
</tr>
<tr>
<td>optional_ie_incorrect</td>
<td>Displays messages with an invalid optional Information Element (IE).</td>
</tr>
<tr>
<td>ie_unexpected</td>
<td>Displays messages with an unexpected Information Element (IE).</td>
</tr>
<tr>
<td>ie_duplicated</td>
<td>Displays messages with a duplicated Information Element (IE).</td>
</tr>
<tr>
<td>total_forwarded</td>
<td>Displays the total messages forwarded.</td>
</tr>
<tr>
<td>signalling_msg_dropped</td>
<td>Displays the total messages dropped.</td>
</tr>
<tr>
<td>signalling_msg_forwarded</td>
<td>Displays the total messages forwarded.</td>
</tr>
<tr>
<td>total_deleted_pdp</td>
<td></td>
</tr>
<tr>
<td>total_deleted_pdpmcb</td>
<td></td>
</tr>
<tr>
<td>total_dup_sig_mcbinfo</td>
<td></td>
</tr>
<tr>
<td>total_dup_data_mcbinfo</td>
<td></td>
</tr>
<tr>
<td>no_new_sgw_sig_mcbinfo</td>
<td></td>
</tr>
<tr>
<td>no_new_sgw_data_mcbinfo</td>
<td></td>
</tr>
</tbody>
</table>

Table 48: GPRS GTP Statistics
<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signalling_msg_dropped</td>
<td>Displays the signaling messages dropped.</td>
</tr>
<tr>
<td>data_msg_dropped</td>
<td>Displays the data messages dropped.</td>
</tr>
<tr>
<td>total_forwarded</td>
<td>Displays the total messages forwarded.</td>
</tr>
<tr>
<td>signalling_msg_forwarded</td>
<td>Displays the signaling messages forwarded.</td>
</tr>
<tr>
<td>data_msg_forwarded</td>
<td>Displays the data messages forwarded.</td>
</tr>
<tr>
<td>total_created_pdp</td>
<td>Displays the total Packet Data Protocol (PDP) or bearer contexts created.</td>
</tr>
<tr>
<td>total_deleted_pdp</td>
<td>Displays the total Packet Data Protocol (PDP) or bearer contexts deleted.</td>
</tr>
<tr>
<td>total_created_pdpmcb</td>
<td>These fields relate to the use of PDP master control blocks, which is an implementation feature. These counters are used by Cisco Technical Support for troubleshooting and are not of direct interest to end users.</td>
</tr>
<tr>
<td>total_deleted_pdpmcb</td>
<td></td>
</tr>
<tr>
<td>total_dup_sig_mcbinfo</td>
<td></td>
</tr>
<tr>
<td>total_dup_data_mcbinfo</td>
<td></td>
</tr>
<tr>
<td>no_new_sgw_sig_mcbinfo</td>
<td></td>
</tr>
<tr>
<td>no_new_sgw_data_mcbinfo</td>
<td></td>
</tr>
<tr>
<td>pdp_non_existent</td>
<td>Displays the messages received for a non-existent PDP context.</td>
</tr>
</tbody>
</table>

The following command displays information about the PDP contexts:

```bash
show service-policy inspect gtp pdp-context
```

The following table describes the output from the `show service-policy inspect gtp pdp-context` command.

**Table 49: PDP Contexts**

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Displays the version of GTP.</td>
</tr>
<tr>
<td>TID</td>
<td>Displays the tunnel identifier.</td>
</tr>
<tr>
<td>MS Addr</td>
<td>Displays the mobile station address.</td>
</tr>
<tr>
<td>Column Heading</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SGSN Addr</td>
<td>Displays the serving gateway service node (SGSN) or serving gateway (SGW).</td>
</tr>
<tr>
<td>SGW Addr</td>
<td></td>
</tr>
<tr>
<td>Idle</td>
<td>Displays the time for which the PDP or bearer context has not been in use.</td>
</tr>
<tr>
<td>APN</td>
<td>Displays the access point name.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear service-policy</td>
<td>Clears all service policy statistics.</td>
</tr>
<tr>
<td>configure inspection</td>
<td>Enables or disables the default inspections.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the service policies configured in the running configuration.</td>
</tr>
<tr>
<td>service-policy</td>
<td></td>
</tr>
</tbody>
</table>
show shun

To display shun information, use the **show shun** command.

`show shun [src_ip | statistics]`

### Syntax Description

- **src_ip** (Optional) Displays the information for that address.
- **statistics** (Optional) Displays the interface shun statistics.

### Command History

- **Release**  
  - **6.1**  
  - This command was introduced.

### Examples

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

```
> show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear shun</td>
<td>Disables all the shuns that are currently enabled and clears the shun statistics.</td>
</tr>
<tr>
<td>shun</td>
<td>Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.</td>
</tr>
</tbody>
</table>
show sip

To display SIP sessions, use the `show sip` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show sip` command displays information for SIP sessions established across the Firepower Threat Defense device.

**Examples**

The following is sample output from the `show sip` command:

```
> show sip
Total: 2
  call-id c3943000-960ca-2e43-228f@10.130.56.44
    | state Call init, idle 0:00:01
  call-id c3943000-860ca-7e1f-11f7@10.130.56.45
    | state Active, idle 0:06:06
```

This sample shows two active SIP sessions on the Firepower Threat Defense device (as shown in the Total field). Each call-id represents a call.

The first session, with the call-id c3943000-960ca-2e43-228f@10.130.56.44, is in the state Call Init, which means the session is still in call setup. Call setup is complete only when the ACK is seen. This session has been idle for 1 second.

The second session is in the state Active, in which call setup is complete and the endpoints are exchanging media. This session has been idle for 6 seconds.

**Related Commands**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show conn</td>
<td>Displays the connection state for different connection types.</td>
</tr>
</tbody>
</table>
show skinny

To displays information for SCCP (Skinny) sessions, use the `show skinny` command.

```bash
show skinny [audio | video]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audio</td>
<td>Show SCCP audio sessions</td>
</tr>
<tr>
<td>video</td>
<td>Show SCCP video sessions</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show skinny` command under the following conditions. There are two active Skinny sessions set up across the device. The first one is established between an internal Cisco IP Phone at local address 10.0.0.11 and an external Cisco Unified Communications Manager at 172.18.1.33. TCP port 2000 is the Cisco Unified Communications Manager. The second one is established between another internal Cisco IP Phone at local address 10.0.0.22 and the same Cisco Unified Communications Manager.

```bash
> show skinny
MED 10.0.0.22/20798 172.18.1.11/22948
LOCAL 10.0.0.11/52238 172.18.1.33/2000 1
  MEDIA 10.0.0.11/22948 172.18.1.22/20798
  MEDIA 10.0.0.22/20798 172.18.1.11/22948
2 10.0.0.22/52232 172.18.1.33/2000 1
  MEDIA 10.0.0.22/20798 172.18.1.11/22948
```

The output indicates a call has been established between both internal Cisco IP Phones. The RTP listening ports of the first and second phones are UDP 22948 and 20798 respectively.

**Related Commands**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show conn</td>
<td>Displays the connection state for different connection types.</td>
</tr>
</tbody>
</table>
show sla monitor

To display information on the Internet Protocol Service Level Agreement (IP SLA), use the `show sla monitor` command.

```
show sla monitor (configuration | operational-state) [sla_id]
```

**Syntax Description**
- `configuration`: Displays the SLA configuration values, including the defaults.
- `operational-state`: Displays the operational state of SLA operations.
- `sla_id` (Optional): The ID number of the SLA operation. Valid values are from 1 to 2147483647.

**Command Default**
If the SLA ID is not specified, the configuration values for all SLA operations are shown.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `show running-config sla monitor` command to see the SLA operation commands in the running configuration.

**Examples**
The following is sample output from the `show sla monitor configuration` command. It displays the configuration values for SLA operation 124. Following the output of the `show sla monitor configuration` command is the output of the `show running-config sla monitor` command for the same SLA operation.

```
> show sla monitor configuration 124
SA Agent, Infrastructure Engine-II
Entry number: 124
Owner: 
Tag: 
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

Cisco Firepower Threat Defense Command Reference 843
show running-config sla monitor 124

sla monitor 124
type echo protocol ipIcmpEcho 10.1.1.1 interface outside
timeout 1000
frequency 3
sla monitor schedule 124 life forever start-time now

The following is sample output from the show sla monitor operational-state command:

show sla monitor operational-state

Entry number: 124
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0  RTTMin: 0  RTTMax: 0
NumOfRTT: 0  RTTSum: 0  RTTSum2: 0

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config sla monitor</td>
<td>Displays the SLA operation configuration commands in the running configuration.</td>
</tr>
</tbody>
</table>
**show snmp-server**

To display information about the SNMP servers configured on the device, use the `show snmp-server` command.

```
show snmp-server { engineID | group | host | statistics | user [username] }
```

**Syntax Description**

- **engineID**: Displays the identification of the SNMP engine.
- **group**: Displays the names of configured SNMP groups, the security model being used, the status of different views, and the storage type of each group.
- **host**: Displays the names of configured SNMP hosts that belong to a host group, the interface being used, and the version of SNMP being used.
- **statistics**: Displays SNMP server statistics.
- **user [username]**: Displays information about the characteristics of SNMP users. You can optionally specify a username to limit the information to that user.

**Command History**

- **6.1**: This command was introduced.

**Usage Guidelines**

An SNMP engine is a copy of SNMP that can reside on a local device. The engine ID is a unique value that is assigned for each SNMP agent. The engine ID is not configurable. The engine ID is 25 bytes long, and is used to generate encrypted passwords. In a failover pair, the engine ID is synchronized with the peer.

SNMP users and groups are used according to the View-based Access Control Model (VACM) for SNMP. The SNMP group determines the security model to be used. The SNMP user should match the security model of the SNMP group. Each SNMP group name and security level pair must be unique.

**Examples**

The following is sample output from the `show snmp-server engineid` command:

```
> show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

The following is sample output from the `show snmp-server group` command:

```
> show snmp-server group
  groupname: public       security model:v1
    readview: <no readview specified>    writeview: <no writeview specified>
    notifyview: <no readview specified>
    row status: active
  groupname: public       security model:v2c
    readview: <no readview specified>    writeview: <no writeview specified>
    notifyview: *<no readview specified>
    row status: active
```
The following is sample output from the `show snmp-server host` command, which shows only the active hosts polling the device:

```
> show snmp-server host
host ip = 10.10.10.3, interface = mgmt poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt poll community ***** version 2c
```

The following is sample output from the `show snmp-server user` command:

```
> show snmp-server user authuser
User name: authuser
Engine ID: 00000009020000000C025808
storage-type: nonvolatile active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

The output provides the following information:

- The username, which is a string that identifies the name of the SNMP user.
- The engine ID, which is a string that identifies the copy of SNMP on the device.
- The storage-type, which indicates whether or not the settings have been set in volatile or temporary memory on the device, or in nonvolatile or persistent memory, in which settings remain after the device has been turned off and on again.
- The active access list, which is the standard IP access list associated with the SNMP user.
- The Rowstatus, which indicates whether or not it is active or inactive.
- The authentication protocol, which identifies which authentication protocol is being used. Options are MD5, SHA, or none. If authentication is not supported in your software image, this field does not appear.
- The privacy protocol, which indicates whether or not DES packet encryption is enabled. If privacy is not supported in your software image, this field does not appear.
- The group name, which indicates to which SNMP group the user belongs. SNMP groups are defined according to the View-based Access Control Model (VACM).

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear snmp-server statistics</td>
<td>Clears the SNMP packet input and output counters.</td>
</tr>
<tr>
<td>show running-config snmp-server</td>
<td>Displays the SNMP server configuration.</td>
</tr>
</tbody>
</table>

---

**show snmp-server**

**Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear snmp-server statistics</td>
<td>Clears the SNMP packet input and output counters.</td>
</tr>
<tr>
<td>show running-config snmp-server</td>
<td>Displays the SNMP server configuration.</td>
</tr>
</tbody>
</table>
**show snort counters**

To display the statistics for the Snort preprocessor connections, use the `show snort counters` command.

```plaintext
show snort counters { action | stream | sip | ssl | smtp } { all | instance x }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>action</th>
<th>Shows instance level statistics of Snort for actions, limits, and verdicts.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>stream</td>
<td>Shows statistics for the stream preprocessor.</td>
</tr>
<tr>
<td></td>
<td>sip</td>
<td>Shows statistics for the SIP preprocessor.</td>
</tr>
<tr>
<td></td>
<td>ssl</td>
<td>Shows statistics for the SSL preprocessor.</td>
</tr>
<tr>
<td></td>
<td>smtp</td>
<td>Shows statistics for the SMTP preprocessor.</td>
</tr>
<tr>
<td></td>
<td>all</td>
<td>Shows statistics for all the Snort instances in the system. For example, <code>show snort counters action all</code>, <code>show snort counters smtp all</code>, and so on.</td>
</tr>
<tr>
<td></td>
<td>instance x</td>
<td>Shows statistics for the selected Snort instance in the system. For example, <code>show snort counters smtp instance 11</code>. Use the <code>show snort instances</code> command to determine the available instance numbers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display statistics for Snort instances in your system. You can use these statistics for informational and debugging purposes. Consult Cisco TAC to help you debug your system with this command. Use the `show snort counters action all` command to view instance level statistics of Snort for actions, limits, and verdicts for all the Snort instances in your system. Use the `show snort instances` command to determine the available instance numbers.

The following example displays instance level statistics of Snort for actions, limits, and verdicts for all the Snort instances in your system.

```
> show snort counters action all
Instance : 1
----------
Action Stats are not available
  Total Action Processed: 0
...

Instance : 16
----------
Action Stats:
  Alerts: 0 ( 0.000%)
```

Cisco Firepower Threat Defense Command Reference
The following example shows stream statistics.

```bash
> show snort counters stream all
Instance : 1
----------
Stream statistics not available
Total sessions: 0
```

```bash
...
Instance : 16
----------
Stream statistics:
  Total sessions: 665
  TCP sessions: 665
  UDP sessions: 0
  ICMP sessions: 0
  IP sessions: 0
  TCP Prunes: 0
  UDP Prunes: 0
  ICMP Prunes: 0
  IP Prunes: 0
  TCP StreamTrackers Created: 0
  TCP StreamTrackers Deleted: 0
  TCP Timeouts: 661
  TCP Segments Queued: 0
  TCP Segments Released: 0
  TCP Rebuilt Packets: 0
  TCP Segments Used: 0
  TCP Discards: 0
  TCP Gaps: 0
  UDP Sessions Created: 0
  UDP Sessions Deleted: 0
  UDP Timeouts: 0
  UDP Discards: 0
  Events: 0
  Internal Events: 0
```
The following example shows SMTP statistics for Snort instance 1.

```
> show snort counters smtp instance 1
Instance : 1
-----------
SMTP Preprocessor Statistics
Total sessions : 80
Max concurrent sessions : 1
Base64 attachments decoded : 0
Total Base64 decoded bytes : 0
Quoted-Printable attachments decoded : 0
Total Quoted decoded bytes : 0
UU attachments decoded : 0
Total UU decoded bytes : 0
Non-Encoded MIME attachments extracted : 0
Total Non-Encoded MIME bytes extracted : 0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear snort statistics</td>
<td>Clears Snort inspection statistics.</td>
</tr>
<tr>
<td>show snort statistics</td>
<td>Displays the number of packets that are matched for various Snort verdicts when traffic is inspected by Snort.</td>
</tr>
<tr>
<td>show snort tls-offload</td>
<td>Displays statistics related to packets encrypted and decrypted by the inspection engine (Snort) in the hardware.</td>
</tr>
</tbody>
</table>
show snort instances

To display a list of the Snort instance numbers, which you can use in other show snort commands, use the show snort instances command.

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Example

The following example displays the list of Snort instances.

```plaintext
> show snort instances
Total number of instances available - 2
+----------+---------+
| INSTANCE | PID     |
+----------+---------+
| 1        | 2787    |
| 2        | 2788    |
+----------+---------+
```
show snort preprocessor-memory-usage

To display memory usage statistics for Snort preprocessors per Snort instance, use the show snort preprocessor-memory-usage command.

show snort preprocessor-memory-usage  instance_ID  {all | imap | pop | smtp}

Syntax Description

| instance_ID | The ID number of the Snort instance. Use the show snort instances command to obtain a list of the instance ID numbers that are active on your system. |
| all | Displays the statistics for all preprocessors. |
| imap | Displays the statistics for the IMAP preprocessor only. |
| pop | Displays the statistics for the POP preprocessor only. |
| smtp | Displays the statistics for the SMTP preprocessor only. |

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Example

The following example displays statistics for the SMTP preprocessor for Snort instance 1. You are prompted for the admin password.

```
> show snort preprocessor-memory-usage 1 smtp

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

Password:

Snort Memory Usage for: Instance-1
----------------------------------

Memory Statistics of SMTP on: Fri Jul 12 09:13:02 2019

SMTP Session Statistics:
  Total Sessions seen: 0
  Max concurrent sessions: 0
  Current Active sessions: 0

Memory Pool:
  Free Memory:
    SMTP Mime Pool: 17968000 bytes
    SMTP Pool: 0 bytes
  Used Memory:
```

Cisco Firepower Threat Defense Command Reference
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Mime Pool:</td>
<td>0 bytes</td>
<td></td>
</tr>
<tr>
<td>SMTP Pool:</td>
<td>0 bytes</td>
<td></td>
</tr>
<tr>
<td>Total Memory:</td>
<td>17968000 bytes</td>
<td></td>
</tr>
<tr>
<td>Session:</td>
<td>0 bytes</td>
<td></td>
</tr>
<tr>
<td>Configuration:</td>
<td>16784 bytes</td>
<td></td>
</tr>
<tr>
<td>Total Memory:</td>
<td>16784 bytes</td>
<td></td>
</tr>
<tr>
<td>No of allocs:</td>
<td>38 times</td>
<td></td>
</tr>
<tr>
<td>IP sessions:</td>
<td>30 times</td>
<td></td>
</tr>
</tbody>
</table>

**show snort preprocessor-memory-usage**
show snort statistics

To display the number of packets that are matched for various Snort verdicts when traffic is inspected by Snort, use the `show snort statistics` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to show Snort inspection results of your access policy and intrusion rule configurations. This command is typically used when debugging unexpected Snort inspection behavior. The statistics include the following:

- **Passed Packets**—The number of packets sent to Snort from Lina.
- **Blocked Packets**—The number of packets blocked in Lina and not sent to Snort.
- **Injected Packets**—The number of packets Snort created and added to the traffic stream. For example, if you configure a block with reset action, Snort generates packets to reset the connection.
- **Packets bypassed (Snort Down or Snort Busy)**—If you configure the system to allow packets that require Snort inspection and Snort cannot perform the inspection, these counters are the number of packets that bypassed inspection when Snort was either down or too busy to handle the packets.

⚠️ **Caution**

When flows are bypassed (passed without inspection) these busy and down counters increment until the bypassed session ends, which can occur even when Snort is no longer busy or down. For example, counters could increment for days if a persistent TCP connection that lasts for days sends a packet while Snort is busy or down and then continues after Snort resumes.

- **Fast-forwarded flows**—The number of flows that were fast forwarded by policy, and thus not inspected.
- **Blacklisted flows**—The number of flows from policy configuration that were dropped by Snort.
- **Start-of-flow events**—The Lina process sends start-of-flow events to Snort when it fast paths a flow without sending it to Snort. These events help Snort keep track of the connections and report the connection events.
- **End-of-flow events**—The Lina process sends end-of-flow events to Snort when a fast path flow ends.
- **Denied flow events**—The Lina process sends denied flow events to Snort when it decides to drop a flow before sending it to Snort.
- **Frames forwarded to Snort before drop**—Valid for NGIPS interfaces only. This is the number of to-be-dropped packets forwarded to Snort. When the Lina process decides to drop the frame for some reason such as (Invalid TCP header length, Invalid UDP length or Invalid IP length), the frames are also sent to Snort for visibility.
- **Inject packets dropped**—The number of packets that Snort added to the traffic stream that were dropped.
Examples

The following sample transcript shows the information displayed by the `show snort statistics` command:

```
show snort statistics
Packet Counters:
   Passed Packets  6
   Blocked Packets 321
   Injected Packets 284
   Packets bypassed (Snort Down) 0
   Packets bypassed (Snort Busy) 0

Flow Counters:
   Fast-Forwarded Flows 0
   Blacklisted Flows 0

Miscellaneous Counters:
   Start-of-Flow events 0
   End-of-Flow events 0
   Denied flow events 0
   Frames forwarded to Snort before drop 0
   Inject packets dropped 0
```

In the following example, consider a case where the access control policy is configured to block and reset on all traffic. Lina cannot handle the reset, so it promotes the packets to Snort to block and inject the reset to both client and server.

- Passed packets—shows eight packets passed from Lina to Snort.
- Injected packets—shows the two packets sent to client and server.
- Blacklisted flows—shows the flows Snort has told Lina to block.

> `show snort statistics`
Packet Counters:
   Passed Packets  8
   Blocked Packets 0
   Injected Packets 2
   Packets bypassed (Snort Down) 0
   Packets bypassed (Snort Busy) 0

Flow Counters:
   Fast-Forwarded Flows 0
   Blacklisted Flows 3

Miscellaneous Counters:
   Start-of-Flow events 0
   End-of-Flow events 0
   Denied flow events 0
   Frames forwarded to Snort before drop 0
   Inject packets dropped 0

Note There are no *blocked* packets in this example.
In the following example, consider a case where the access control policy has one rule that matches an FTP port and has a block action, and another rule that matches an HTTP application and has an allow action.

- Passed packets—shows 60 HTTP packets because Lina sends packets for allow rules to Snort.
- Denied flow events—shows two data and control channel packets that Lina handled with an FTP port match.

Note: There are no blocked packets in this example.

```
> show snort statistics
Packet Counters:
Passed Packets       60
Blocked Packets      0
Injected Packets     0
Packets bypassed (Snort Down) 0
Packets bypassed (Snort Busy) 0

Flow Counters:
Fast-Forwarded Flows 0
Blacklisted Flows    0

Miscellaneous Counters:
Start-of-Flow events 0
End-of-Flow events   0
Denied flow events   2
Frames forwarded to Snort before drop 0
Inject packets dropped 0
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear snort statistics</td>
<td></td>
<td>Clears Snort inspection statistics.</td>
</tr>
<tr>
<td>configure snort preserve-connection</td>
<td></td>
<td>Determine whether to preserve existing TCP/UDP connections on routed and transparent interfaces in case the Snort process goes down.</td>
</tr>
</tbody>
</table>
show snort tls-offload

To display statistics related to packets encrypted and decrypted by the inspection engine (Snort) in hardware, use the `show snort tls-offload` command. This command is available only on the following managed devices, which support SSL hardware acceleration:

- Firepower 2100 with Firepower Threat Defense
- Firepower 4100/9300 with Firepower Threat Defense

For information about TLS crypto acceleration support on Firepower 4100/9300 FTD container instances, see the FXOS Configuration Guide.

TLS crypto acceleration is not supported on any virtual appliances or on any hardware except for the preceding.

show snort tls-offload [proxy | tracker | description]

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy</td>
<td>(Optional.) Shows statistics for the proxy only.</td>
</tr>
<tr>
<td>tracker</td>
<td>(Optional.) Shows statistics for the tracker only.</td>
</tr>
<tr>
<td>description</td>
<td>(Optional.) Shows descriptions of the counters for both the proxy and the tracker.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display detailed statistics for Snort's proxy and tracker components. You can use these statistics for informational and debugging purposes. Use the `show snort tls-offload description` command to view a description of the counters. Consult Cisco TAC to help you debug your system with this command.

Following is an example `show snort tls-offload` command:

```
====== Tracker Statistics ======
TOTAL_CONNECTION 2774
TOTAL_RSA_KEY_EXCHANGE_4K 2774
TOTAL_CIPHER_SUITE_ENCR_AES 2774
TOTAL_CIPHER_SUITE_HASH_SHA1 2774
TOTAL_CKE_PMS_DECRYPTED 2774
TOTAL_RECORD_DECRYPTED 363001
TOTAL_RECORD_ENCRYPTED 363001
TOTAL_CONNECTION_W_DUR (<0.5s) 2771
AVG_CONNECTION_DURATION (ms) 184
AVG_HANDSHAKE_TIME (ms) 37
AVG_CKE_PMS_DECRYPT_TIME (us) 21402
AVG_RECORD_DECRYPT_TIME (us) 619
AVG_RECORD_ENCRYPT_TIME (us) 477
PEAK_CONNECTION_DURATION (ms) 400
PEAK_HANDSHAKE_TIME (ms) 62
CONCURRENT_CONNECTION/Peak 3/3
CPS_ATTEMPTED/Peak 7/8
CPS_COMPLETED/Peak 8/8
CKE_PMS_DECRYPTING_Q/Peak 0/2
SKE_DH_PARAM_SIGNING_Q/Peak 0/0
```
RECORD_ENCRYPTING_Q/Peak 1/25
RECORD_DECRYPTING_Q/Peak 1/2

----- Proxy Statistics -----
TOTAL_CONNECTION(LW+FP) 15855
TOTAL_CONNECTION_FP 15853
CONNECTION_FP_RECV_FIN 31697
CONNECTION_FP_RECV_RST 27
CONNECTION_LW_RECV_FIN 2
CONCURRENT_CONNECTION_LW/Peak 0/2
CONCURRENT_CONNECTION_FP/Peak 3/7
BYPASS_NOT_ENOUGH_MEM 0

--- Related Commands ---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear snort tls-offload</td>
<td>Clear statistics counters.</td>
</tr>
<tr>
<td>debug snort tls-offload</td>
<td>Displays error debug messages of all types for all Snort processes.</td>
</tr>
</tbody>
</table>
show software authenticity

To show software authenticity information, use the `show software authenticity` command.

```
show software authenticity { development | file filename | keys | running }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>development</th>
<th>Displays whether the loading of development key signed images is enabled or disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>file filename</code></td>
<td>Displays digital signature information related to software authentication for a specific image file.</td>
</tr>
<tr>
<td></td>
<td>keys</td>
<td>Displays information about development keys and release keys that are stored in SPI flash.</td>
</tr>
<tr>
<td></td>
<td>running</td>
<td>Displays digital signature information related to software authentication for the currently running image file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>The output for files and the running image provides the following information.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The filename, which is the name of the filename in memory.</td>
</tr>
<tr>
<td></td>
<td>• The image type, which is the type of image being shown.</td>
</tr>
<tr>
<td></td>
<td>• The signer information specifies the signature information, which includes the following:</td>
</tr>
<tr>
<td></td>
<td>• The common name, which is the name of the software manufacturer.</td>
</tr>
<tr>
<td></td>
<td>• The organization unit, which indicates the hardware that the software image is deployed on.</td>
</tr>
<tr>
<td></td>
<td>• The organization name, which is the owner of the software image.</td>
</tr>
<tr>
<td></td>
<td>• The certificate serial number, which is the certificate serial number for the digital signature.</td>
</tr>
<tr>
<td></td>
<td>• The hash algorithm, which indicates the type of hash algorithm used in digital signature verification.</td>
</tr>
<tr>
<td></td>
<td>• The signature algorithm, which identifies the type of signature algorithm used in digital signature verification.</td>
</tr>
<tr>
<td></td>
<td>• The key version, which indicates the key version used for verification.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show software authenticity development` command:

```
> show software authenticity development
Loading of development images is disabled
```
The following is sample output from the `show software authenticity file` command. In this example, the file is a development image. You would see the same output for `show software authenticity running` about the image file that is currently running on the device.

```plaintext
> show software authenticity file os.img
File Name : disk0:/os.img
Image type : Development
Signer Information:
  Common Name : abraxas
  Organization Unit : NCS_KentonASA
  Organization Name : CiscoSystems
  Certificate Serial Number : 57F4610F
  Hash Algorithm : SHA2 512
  Signature Algorithm : 2048-bit RSA
  Key Version : A

The following is sample output from the `show software authenticity keys` command.

```plaintext
> show software authenticity keys
Public Key #1 Information
------------------------------------
Key Type : Release (Primary)
Public Key Algorithm : 2048-bit RSA
Modulus :
Exponent :
65537
Key Version : A
Public Key #2 Information
------------------------------------
Key Type : Development (Primary)
Public Key Algorithm : 2048-bit RSA
Modulus :
05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
```
Exponent : 65537
Key Version : A
Public Key #3 Information
--------------
Key Type : Release (Backup)
Public Key Algorithm : 2048-bit RSA
Modulus :
Exponent : 65537
Key Version : A
Public Key #4 Information
--------------
Key Type : Development (Backup)
Public Key Algorithm : 2048-bit RSA
Modulus :
Exponent : 65537
Key Version : A
Related Commands
Command | Description
--------|-------------------
show version | Displays the software version, hardware configuration, license key, and related uptime data.
show ssh-access-list

To show the SSH access list settings for the management interface, use the `show ssh-access-list` command.

**show ssh-access-list**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to show SSH access list settings for the management interface. The access list determines from which IP addresses users can attempt SSH connections to the management IP address. This list does not control SSH access to any data interface.

**Examples**

The following sample is default output from the `show ssh-access-list` command. This access list allows SSH connections to the management IP address from any IP address. Any user must supply a valid username/password to actually complete the SSH connection.

```
> show ssh-access-list
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh
ACCEPT tcp anywhere anywhere anywhere state NEW tcp dpt:ssh
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure ssh-access-list</code></td>
<td>Configure the SSH access list for the management interface.</td>
</tr>
</tbody>
</table>
show ssl

To display information about the active SSL sessions and available ciphers, use the show ssl command.

show ssl [cache | ciphers [level] | errors [trace] | mib [64] | objects]

**Syntax Description**

- **cache** (Optional) Displays SSL session cache statistics.
- **ciphers [level]** (Optional) Displays SSL ciphers available for use. Include the level keyword to view only those ciphers available for the given level, which indicates cipher strength. The following are the possible levels in increasing order of strength:
  - *all*
  - *low*
  - *medium* (This is the default if you do not specify a level)
  - *fips*
  - *high* (applies to TLSv1.2 only)
- **errors [trace]** (Optional) Displays SSL errors. Include the trace keyword to include trace information for each error.
- **mib [64]** (Optional) Displays SSL MIB statistics. Include the 64 keyword to see 64-bit counter statistics.
- **objects** (Optional) Displays SSL object statistics.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command shows information about the current SSLv3 or greater sessions, including the enabled cipher order, which ciphers are disabled, SSL trustpoints being used, and whether certificate authentication is enabled. These settings are for SSL connections on the data interfaces, not on the management interface.

**Examples**

The following is sample output from the show ssl command:

```
> show ssl
Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
Self-signed (RSA 2048 bits RSA-SHA256) certificate available
Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
```
Certificate authentication is not enabled

The following is sample output from the `show ssl ciphers` command.

```
> show ssl ciphers
Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DES-CBC3-SHA
tls1v (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tls1v.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tls1v.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
dts1v (medium):
```
show ssl

DHE-RSA-AES256-SHA
AES256-SHA
DHE-RSA-AES128-SHA
AES128-SHA
DES-CBC3-SHA
show ssl-policy-config

To display information about the currently applied SSL policy configuration, including policy description, default logging settings, all enabled SSL rules and rule configurations, trusted CA certificates, and undecryptable traffic actions, use the `show ssl-policy-config` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You configure the SSL policy in Firepower Management Center and attach it to the access control policy assigned to a device. You can use this command to view information on the actions configured for SSL decryption on traffic that passes through the device.

**Examples**

The following example shows what appears if you have not configured an SSL policy for the device.

```
> show ssl-policy-config
SSL policy not yet applied.
```

The following example shows a configured SSL policy.

```
> show ssl-policy-config
------------------------[ General SSL Policy ]------------------------

------------------------[ Default Action ]------------------------
Default Action : Do Not Decrypt

--------[ Category: admin_category (Built-in) ]--------

--------[ Category: standard_category (Built-in) ]------

--------[ Block unwanted applications ]--------
State : Enabled
Action : Block
Source Zones : outside_zone
Destination Zones : dmz_zone
Applications : HTTP/SSL Tunnel (3860)

--------[ Category: root_category (Built-in) ]--------

--------[ Trusted CA Certificates ]--------
Cisco-Trusted-Authorities (group)
thawte-Primary-Root-CA
UTN-DATACorp-SGC
Chambers-of-Commerce-Root-2008
Izenpe.com-1
A-Trust-Qual-02
A-Trust-nQual-03
Common-Policy
```
show ssl-policy-config

Starfield-Root-Certificate-Authority-G2
GeoTrust-Primary-Certification-Authority
Certum-Trusted-Network-CA
UTN-USERFirst-Object
C_US-O_VeriSign-Inc.-OU_Class-3-Public-Primary-Certification-Authority-G2-OU_c-1998-VeriSign-Inc.-For-authorized-use-only-OU_VeriSign-Trust-Network-CA-Disig-Root-R1
C_US-O_Equifax-OU_Equifax-Secure-Certificate-Authority
Thawte-Server-CA-1
VeriSign-Class-3-Public-Primary-Certification-Authority-G3
COMODO-Certification-Authority
VeriSign-Class-3-Public-Primary-Certification-Authority-G5
UTN-USERFirst-Client-Authentication-and-Email
TC-TrustCenter-Universal-CA-III
Cisco-Root-CA-2048
Staat-der-Nederlanden-Root-CA-G2

(...Remaining trusted CA certificates removed...)

-------------[ Undecryptable Actions ]--------------
Unsupported Cipher Suite : Inherit Default Action
Unknown Cipher Suite : Inherit Default Action
Compressed Session : Inherit Default Action
Uncached Session ID : Inherit Default Action
SSLv2 Session : Inherit Default Action
Handshake Error : Inherit Default Action
Decryption Error : Block

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Shows information about the currently configure access control policy.</td>
</tr>
<tr>
<td>access-policy-config</td>
<td>Shows information about the currently configure access control policy.</td>
</tr>
</tbody>
</table>
show ssl-protocol

To show the SSL protocols currently configured for HTTPS access to the local device manager (Firepower Device Manager), use the **show ssl-protocol** command.

```plaintext
show ssl-protocol
```

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to view the SSL protocols configured for the management interface. These are the allowed protocols for HTTPS connections, which are used to open the local manager, Firepower Device Manager. These protocols are not used for remote managers.

Use the **configure ssl-protocol** command to configure these protocols.

**Examples**

The following example shows how to view the SSL protocols currently defined when using the local manager.

```plaintext
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure ssl-protocol</td>
<td>Configures the SSL protocols for HTTPS access to the management interface.</td>
</tr>
</tbody>
</table>
show startup-config

To show the startup configuration or to show any errors when the startup configuration loaded, use the `show startup-config` command.

`show startup-config [errors]`

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>errors</code></td>
<td>(Optional) Shows any errors that were generated when the startup configuration loaded.</td>
</tr>
</tbody>
</table>

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

The `show startup-config` command displays the startup system configuration. You cannot directly configure these commands. Instead, they are configured by the manager controlling the device, for example, Firepower Management Center or Firepower Device Manager.

However, this is a partial configuration. It shows what can be configured using ASA Software configuration commands only, although some commands might be specific to Firepower Threat Defense. These commands are ported to Firepower Threat Defense. Thus, you should use the information in the startup configuration as a troubleshooting aid only. Use the device manager as the main means to analyze the device configuration.

## Examples

The following is sample output from the `show startup-config` command:

```
> show startup-config
: Saved

: Serial Number: JAD192100RG
: Hardware: ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
: Written by enable_1 at 20:39:10.749 UTC Tue Jun 28 2016

NGFW Version 6.1.0
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted names

{...Output Truncated...}
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Shows the running configuration.</td>
</tr>
</tbody>
</table>
show summary

To display a summary of the most commonly used information (version, type, UUID, and so on) about the device, use the show summary command.

```
show summary
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Summary information includes basic show version output, plus a list of applied policies and Snort version information.

### Examples

The following is an example of showing summary information.

```
> show summary
--------[ ftd1.example.com ]---------
Model : Cisco ASA5512-X Threat Defense (75) Version 6.1.0 (Build 2007)
UUID  : 703006f4-8ff6-11e6-bb6e-8f2d5feb243
Rules update version : 2016-03-28-001-vrt
VDB version : 271
----------------------------------------

------------------[ policy info ]-------------------
Access Control Policy : Initial AC Policy
Intrusion Policy      : Balanced Security and Connectivity

----------------------------------------

------------------[ snort version info ]------------------
Snort Version : 2.9.10 GRE (Build 20)
libpcap Version : 1.1.1
PCRE Version    : 7.6 2008-01-28
ZLIB Version    : 1.2.8
----------------------------------------
```
show sunrpc-server active

To display the pinholes open for Sun RPC services, such as NFS and NIS, use the `show sunrpc-server active` command.

```
show sunrpc-server active
```

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show sunrpc-server active` command:

```
> show sunrpc-server active
LOCAL        FOREIGN     SERVICE TIMEOUT
-------------------------------
192.168.100.2/0 209.165.200.5/32780 100005 00:10:00
```

The entry in the LOCAL column shows the IP address of the client or server on the inside interface, while the value in the FOREIGN column shows the IP address of the client or server on the outside interface.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear sunrpc-server active</td>
<td>Clears the pinholes opened for Sun RPC services, such as NFS or NIS.</td>
</tr>
<tr>
<td>show running-config sunrpc-server</td>
<td>Displays information about the SunRPC services configuration.</td>
</tr>
</tbody>
</table>
show switch mac-address-table

To view the switch MAC address table, use the `show switch mac-address-table` command.

---

### Note

Supported for the Firepower 1010 only.

---

**show switch mac-address-table**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The switch MAC address table maintains the MAC address-to-switch port mapping for traffic within each VLAN in the switch hardware. The bridge MAC address table maintains the MAC address-to-VLAN interface mapping for traffic that passes between VLANs.

MAC address entries age out in 5 minutes.

**Examples**

The following is sample output from the `show switch mac-address-table` command.

```
> show switch mac-address-table
Legend: Age - entry expiration time in seconds
Mac Address    | VLAN | Type       | Age | Port
----------------|------|------------|-----|-------
000e.0c4e.2aa4 | 0001 | dynamic    | 287 | Et1/1
0012.d927.fb03 | 0001 | dynamic    | 287 | Et1/1
0013.c4ca.8a8c | 0001 | dynamic    | 287 | Et1/1
00b0.6486.0c14 | 0001 | dynamic    | 287 | Et1/1
00d0.2bff.449f | 0001 | static     | -   | In0/1
0100.5e00.000d | 0001 | static multicast | - | In0/1,Et1/1-8
Total Entries: 6
```

The following table shows each field description:

**Table 50: show switch mac-address-table Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Address</td>
<td>Shows the MAC address.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Shows the VLAN associated with the MAC address.</td>
</tr>
<tr>
<td>Type</td>
<td>Shows if the MAC address was learned dynamically, as a static multicast address, or statically. The only static entry is for the internal backplane interface.</td>
</tr>
<tr>
<td>Age</td>
<td>Shows the age of a dynamic entry in the MAC address table.</td>
</tr>
<tr>
<td>Port</td>
<td>Shows the switch port through which the host with the MAC address can be reached.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show switch vlan</td>
<td>Shows the VLAN and physical MAC address association.</td>
</tr>
</tbody>
</table>
show switch vlan

To view the VLANs and the associated switch ports, use the `show switch vlan` command.

**Note**

Supported for the Firepower 1010 only.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is for models with built-in switches only. For other models, use the `show vlan` command.

**Examples**

The following is sample output from the `show switch vlan` command.

```plaintext
> show switch vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>inside</td>
<td>up</td>
<td>Et1/1, Et1/2</td>
</tr>
<tr>
<td>200</td>
<td>outside</td>
<td>up</td>
<td>Et1/8</td>
</tr>
<tr>
<td>300</td>
<td>-</td>
<td>down</td>
<td>Et1/2, Et1/3</td>
</tr>
<tr>
<td>400</td>
<td>backup</td>
<td>down</td>
<td>Et1/4</td>
</tr>
</tbody>
</table>
```

The following table shows each field description:

**Table 51: show switch vlan Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Shows the VLAN number.</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the name of the VLAN interface. If no name is set, or if there is no VLAN interface, the display shows a dash (-).</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the status, up or down, to receive and send traffic to and from the VLAN in the switch. At least one switch port in the VLAN needs to be in an up state for the VLAN state to be up.</td>
</tr>
<tr>
<td>Ports</td>
<td>Shows the switch ports assigned to each VLAN. If a switch port is listed for multiple VLANs, it is a trunk port. The above sample output shows Ethernet 1/2 is a trunk port that carries VLAN 100 and 300.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show switch mac-address-table</code></td>
<td>Shows the switch MAC address table.</td>
</tr>
</tbody>
</table>
show tcpstat

To display the status of the TCP stack and the TCP connections that are terminated on the device (for debugging), use the `show tcpstat` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show tcpstat` command allows you to display the status of the TCP stack and TCP connections that are terminated on the device. The TCP statistics displayed are described in the following table.

**Table 52: TCP Statistics in the show tcpstat Command**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcb_cnt</td>
<td>Number of TCP users.</td>
</tr>
<tr>
<td>proxy_cnt</td>
<td>Number of TCP proxies. TCP proxies are used by user authorization.</td>
</tr>
<tr>
<td>tcp_xmt pkts</td>
<td>Number of packets that were transmitted by the TCP stack.</td>
</tr>
<tr>
<td>tcp_rcv good pkts</td>
<td>Number of good packets that were received by the TCP stack.</td>
</tr>
<tr>
<td>tcp_rcv drop pkts</td>
<td>Number of received packets that the TCP stack dropped.</td>
</tr>
<tr>
<td>tcp bad chksum</td>
<td>Number of received packets that had a bad checksum.</td>
</tr>
<tr>
<td>tcp user hash add</td>
<td>Number of TCP users that were added to the hash table.</td>
</tr>
<tr>
<td>tcp user hash add dup</td>
<td>Number of times a TCP user was already in the hash table when trying to add a new user.</td>
</tr>
<tr>
<td>tcp user srch hash hit</td>
<td>Number of times a TCP user was found in the hash table when searching.</td>
</tr>
<tr>
<td>tcp user srch hash miss</td>
<td>Number of times a TCP user was not found in the hash table when searching.</td>
</tr>
<tr>
<td>tcp user hash delete</td>
<td>Number of times that a TCP user was deleted from the hash table.</td>
</tr>
<tr>
<td>tcp user hash delete miss</td>
<td>Number of times that a TCP user was not found in the hash table when trying to delete the user.</td>
</tr>
<tr>
<td>lip</td>
<td>Local IP address of the TCP user.</td>
</tr>
<tr>
<td>fip</td>
<td>Foreign IP address of the TCP user.</td>
</tr>
<tr>
<td>lp</td>
<td>Local port of the TCP user.</td>
</tr>
<tr>
<td>fp</td>
<td>Foreign port of the TCP user.</td>
</tr>
</tbody>
</table>
### Statistic

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>st</td>
<td>State (see RFC 793) of the TCP user. The possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>1 CLOSED</td>
</tr>
<tr>
<td></td>
<td>2 LISTEN</td>
</tr>
<tr>
<td></td>
<td>3 SYN_SENT</td>
</tr>
<tr>
<td></td>
<td>4 SYN_RCVD</td>
</tr>
<tr>
<td></td>
<td>5 ESTABLISHED</td>
</tr>
<tr>
<td></td>
<td>6 FIN_WAIT_1</td>
</tr>
<tr>
<td></td>
<td>7 FIN_WAIT_2</td>
</tr>
<tr>
<td></td>
<td>8 CLOSE_WAIT</td>
</tr>
<tr>
<td></td>
<td>9 CLOSING</td>
</tr>
<tr>
<td></td>
<td>10 LAST_ACK</td>
</tr>
<tr>
<td></td>
<td>11 TIME_WAIT</td>
</tr>
<tr>
<td>reqlen</td>
<td>Length of the retransmit queue of the TCP user.</td>
</tr>
<tr>
<td>inqlen</td>
<td>Length of the input queue of the TCP user.</td>
</tr>
<tr>
<td>tw_timer</td>
<td>Value of the time_wait timer (in milliseconds) of the TCP user.</td>
</tr>
<tr>
<td>to_timer</td>
<td>Value of the inactivity timeout timer (in milliseconds) of the TCP user.</td>
</tr>
<tr>
<td>cl_timer</td>
<td>Value of the close request timer (in milliseconds) of the TCP user.</td>
</tr>
<tr>
<td>per_timer</td>
<td>Value of the persist timer (in milliseconds) of the TCP user.</td>
</tr>
<tr>
<td>rt_timer</td>
<td>Value of the retransmit timer (in milliseconds) of the TCP user.</td>
</tr>
<tr>
<td>tries</td>
<td>Retransmit count of the TCP user.</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to display the status of the TCP stack.

```plaintext
> show tcpstat
tcb_cnt 2 12 320
proxy_cnt 0 0 160
tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0
lip = 203.0.113.45 fip = 192.0.2.12 lp = 443 fp = 2567 st = 4 reqlen = 0
in0
    tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
    rt_timer = 0 tries 0
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show conn</td>
<td>Displays the connections used and those that are available.</td>
</tr>
</tbody>
</table>
show tech-support

To display the information that is used for diagnosis by technical support analysts, use the `show tech-support` command.

**show tech-support**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `show tech-support` command lets you list information that technical support analysts need to help you diagnose problems.

### Examples

The following example shows how to display information that is used for technical support analysis. The output is shortened to show only its beginning.

```
> show tech-support

--------------[ ftd1.example.com ]--------------
Model         : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build 226)
UUID          : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version : 2016-03-28-001-vrt
VDB version   : 270

Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 3 days 16 hours

Hardware: ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 0 Oxfed01000, 16384KB
Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)
(...Remaining output truncated...)
show threat-detection memory

To show the memory used by advanced threat detection statistics, which are enabled by the threat-detection statistics command in the running configuration, use the show threat-detection memory command.

show threat-detection memory

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Some statistics can use a lot of memory and can affect system performance. This command lets you monitor memory usage so you can adjust your configuration if necessary.

Use FlexConfig to configure the threat-detection statistics command.

Examples

The following is sample output from the show threat-detection memory command:

> show threat-detection memory
Cached chunks:

<table>
<thead>
<tr>
<th>CACHE TYPE</th>
<th>BYTES USED</th>
</tr>
</thead>
<tbody>
<tr>
<td>TD Host</td>
<td>70245888</td>
</tr>
<tr>
<td>TD Port</td>
<td>2724</td>
</tr>
<tr>
<td>TD Protocol</td>
<td>1476</td>
</tr>
<tr>
<td>TD ACE</td>
<td>728</td>
</tr>
<tr>
<td>TD Shared counters</td>
<td>14256</td>
</tr>
</tbody>
</table>

Subtotal TD Chunks 70265072

Regular memory

<table>
<thead>
<tr>
<th></th>
<th>BYTES USED</th>
</tr>
</thead>
<tbody>
<tr>
<td>TD Port</td>
<td>33824</td>
</tr>
<tr>
<td>TD Control block</td>
<td>162064</td>
</tr>
</tbody>
</table>

Subtotal Regular Memory 195888

Total TD memory: 70460960

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config all threat-detection</td>
<td>Shows the threat detection configuration, including the default rate settings if you did not configure them individually.</td>
</tr>
<tr>
<td>show threat-detection statistics host</td>
<td>Shows the host statistics.</td>
</tr>
<tr>
<td>show threat-detection statistics port</td>
<td>Shows the port statistics.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td><code>show threat-detection statistics protocol</code></td>
<td>Shows the protocol statistics.</td>
</tr>
<tr>
<td><code>show threat-detection statistics top</code></td>
<td>Shows the top 10 statistics.</td>
</tr>
</tbody>
</table>
show threat-detection rate

When you enable basic threat detection using the `threat-detection basic-threat` command (using FlexConfig), you can view statistics using the `show threat-detection rate` command.

```
show threat-detection rate  [min-display-rate  events_per_second]  [acl-drop  |  bad-packet-drop  |  conn-limit-drop  |  dos-drop  |  fw-drop  |  icmp-drop  |  inspect-drop  |  interface-drop  |  scanning-threat  |  syn-attack]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl-drop</td>
<td>(Optional) Shows the rate for dropped packets caused by denial by access lists.</td>
</tr>
<tr>
<td>bad-packet-drop</td>
<td>(Optional) Shows the rate for dropped packets caused by denial by a bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length).</td>
</tr>
<tr>
<td>conn-limit-drop</td>
<td>(Optional) Shows the rate for dropped packets caused by the connection limits being exceeded (both system-wide resource limits, and limits set in the configuration).</td>
</tr>
<tr>
<td>dos-drop</td>
<td>(Optional) Shows the rate for dropped packets caused by a detected DoS attack (such as an invalid SPI, Stateful Firewall check failure).</td>
</tr>
<tr>
<td>fw-drop</td>
<td>(Optional) Shows the rate for dropped packets caused by basic firewall check failure. This option is a combined rate that includes all firewall-related packet drops in this command. It does not include non-firewall-related drops such as interface-drop, inspect-drop, and scanning-threat.</td>
</tr>
<tr>
<td>icmp-drop</td>
<td>(Optional) Shows the rate for dropped packets caused by denial by suspicious ICMP packets detected.</td>
</tr>
<tr>
<td>inspect-drop</td>
<td>(Optional) Shows the rate limit for dropped packets caused by packets failing application inspection.</td>
</tr>
<tr>
<td>interface-drop</td>
<td>(Optional) Shows the rate limit for dropped packets caused by an interface overload.</td>
</tr>
<tr>
<td>min-display-rate</td>
<td>(Optional) Limits the display to statistics that exceed the minimum display rate in events per second, from 0 to 2147483647.</td>
</tr>
<tr>
<td>scanning-threat</td>
<td>(Optional) Shows the rate for dropped packets caused by a scanning attack detected. This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.</td>
</tr>
<tr>
<td>syn-attack</td>
<td>(Optional) Shows the rate for dropped packets caused by an incomplete session, such as TCP SYN attack or UDP session with no return data attack.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger.
- The number of times the rates were exceeded.
- The total number of events over the fixed time periods.

The system computes the event counts 30 times over the average rate interval; in other words, the system checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 10 minutes, then the burst interval is 10 seconds. If the last burst interval was from 3:00:00 to 3:00:10, and you use the `show` command at 3:00:15, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the system calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the `show threat-detection rate` command:

```
> show threat-detection rate

<table>
<thead>
<tr>
<th></th>
<th>Average(eps)</th>
<th>Current(eps)</th>
<th>Trigger</th>
<th>Total events</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-min ACL drop:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>16</td>
</tr>
<tr>
<td>1-hour ACL drop:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>112</td>
</tr>
<tr>
<td>1-hour SYN attck:</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>21438</td>
</tr>
<tr>
<td>10-min Scanning:</td>
<td>0</td>
<td>0</td>
<td>29</td>
<td>193</td>
</tr>
<tr>
<td>1-hour Scanning:</td>
<td>106</td>
<td>0</td>
<td>10</td>
<td>384776</td>
</tr>
<tr>
<td>1-hour Bad pkts:</td>
<td>76</td>
<td>0</td>
<td>2</td>
<td>274690</td>
</tr>
<tr>
<td>10-min Firewall:</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>22</td>
</tr>
<tr>
<td>1-hour Firewall:</td>
<td>76</td>
<td>0</td>
<td>2</td>
<td>274844</td>
</tr>
<tr>
<td>10-min DoS attck:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>1-hour DoS attck:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>42</td>
</tr>
<tr>
<td>10-min Interface:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>204</td>
</tr>
<tr>
<td>1-hour Interface:</td>
<td>88</td>
<td>0</td>
<td>0</td>
<td>318225</td>
</tr>
</tbody>
</table>
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear threat-detection rate</td>
<td>Clears basic threat detection statistics.</td>
</tr>
<tr>
<td>show running-config all threat-detection</td>
<td>Shows the threat detection configuration, including the default rate settings if you did not configure them individually.</td>
</tr>
<tr>
<td>show threat-detection statistics</td>
<td>Shows statistics for threat detection.</td>
</tr>
</tbody>
</table>
show threat-detection scanning-threat

If you enable scanning threat detection with the `threat-detection scanning-threat` command (using FlexConfig), then view the hosts that are categorized as attackers and targets using the `show threat-detection scanning-threat` command.

**show threat-detection scanning-threat [attacker | target]**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attacker</td>
<td>(Optional) Shows attacking host IP addresses.</td>
</tr>
<tr>
<td>target</td>
<td>(Optional) Shows targeted host IP addresses.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show threat-detection scanning-threat` command:

```
> show threat-detection scanning-threat
Latest Target Host & Subnet List:
  192.168.1.0 (l2l)
  192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
  192.168.10.234 (outside)
  192.168.10.0 (outside)
  192.168.10.2 (outside)
  192.168.10.3 (outside)
  192.168.10.4 (outside)
  192.168.10.5 (outside)
  192.168.10.6 (outside)
  192.168.10.7 (outside)
  192.168.10.8 (outside)
  192.168.10.9 (outside)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear threat-detection</td>
<td>Clears the list of scanning threat attackers and targets.</td>
</tr>
<tr>
<td>scanning-threat</td>
<td></td>
</tr>
<tr>
<td>show running-config all threat-detection</td>
<td>Shows the threat detection configuration, including the default rate settings if you did not configure them individually.</td>
</tr>
<tr>
<td>show threat-detection statistics</td>
<td>Shows statistics for threat detection.</td>
</tr>
<tr>
<td>shun</td>
<td>Blocks connections from specified hosts, such as scanning threat attackers.</td>
</tr>
</tbody>
</table>
show threat-detection shun

If you enable scanning threat detection with the `threat-detection scanning-threat` command (using FlexConfig), and you automatically shun attacking hosts, then view the currently shunned hosts using the `show threat-detection shun` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To release a host from being shunned, use the `clear threat-detection shun` command.

### Examples

The following is sample output from the `show threat-detection shun` command:

```
> show threat-detection shun
Shunned Host List:  
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear threat-detection shun</td>
<td>Clears the list of automatically shunned hosts.</td>
</tr>
<tr>
<td>show running-config all threat-detection</td>
<td>Shows the threat detection configuration, including the default rate settings if you did not configure them individually.</td>
</tr>
<tr>
<td>show threat-detection scanning-threat</td>
<td>Shows the scanning threat attackers and targets.</td>
</tr>
<tr>
<td>show threat-detection statistics</td>
<td>Shows statistics for threat detection.</td>
</tr>
<tr>
<td>shun</td>
<td>Blocks connections from specified hosts, such as scanning threat attackers.</td>
</tr>
</tbody>
</table>
show threat-detection statistics

If you enable threat statistics with the `threat-detection statistics` command (using FlexConfig), view the statistics using the `show threat-detection statistics` command. For clarity, the major keywords and options are shown separately in the following diagram.

```
show threat-detection statistics [min-display-rate eps] host [ip_address [mask]]
show threat-detection statistics [min-display-rate eps] port [start_port[-end_port]]
show threat-detection statistics [min-display-rate eps] protocol [number | name]
show threat-detection statistics [min-display-rate eps] top [access-list | host | port-protocol] [rate-1 | rate-2 | rate-3] | tcp-intercept [all] [detail] [long]
```

**Syntax Description**

- **host [ip_address [mask]]**
  - Shows host statistics. You can optionally specify an IP address to show statistics for a particular host. You can include the subnet mask for the host.
  - Enable host statistics by configuring the `threat-detection statistics host` command using FlexConfig.

- **min-display-rate eps**
  - (Optional) Limits the display to statistics that exceed the minimum display rate in events per second, between 0 and 2147483647.

- **port [start_port[-end_port]]**
  - Shows TCP/UDP port statistics. You can optionally specify a single port or a range of ports, between 0 and 65535.
  - Enable port statistics by configuring the `threat-detection statistics port` command using FlexConfig.

- **protocol [number | name]**
  - Shows protocol statistics. You can optionally specify the protocol by number or name. The number can be 0 - 255. The name can be one of the following: ah, eigrp, esp, gre, icmp, igmp, igrp, ip, ipinip, ipsec, nos, ospf, pcp, pim, pptp, snp, tcp, udp.
  - Enable protocol statistics by configuring the `threat-detection statistics protocol` command using FlexConfig.
show threat-detection statistics

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>top [access-list</td>
<td>host</td>
</tr>
<tr>
<td>- access-list shows the top 10 ACEs that that match packets, including both permit and deny ACEs. If you enable basic threat detection using the threat-detection basic-threat command, you can track access list denies using the show threat-detection rate access-list command.</td>
<td></td>
</tr>
<tr>
<td>- host shows the top 10 host statistics for each fixed time period. Due to the threat detection algorithm, an interface used for a failover link or state link could appear as one of the top 10 hosts. This occurrence is more likely when you use one interface for both the failover and state link. This is expected behavior, and you can ignore this IP address in the display.</td>
<td></td>
</tr>
<tr>
<td>- port-protocol shows the top 10 combined statistics of TCP/UDP port and IP protocol types. TCP (protocol 6) and UDP (protocol 17) are not included in the display for IP protocols.</td>
<td></td>
</tr>
<tr>
<td>- rate-1, rate-2, rate-3 shows the statistics for the specified fixed rate period only, with 1 being the smallest, 3 the largest intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then rate 1 is 1 hour, rate 2 is 8 hours, and rate 3 is 24 hours.</td>
<td></td>
</tr>
<tr>
<td>top tcp-intercept [all] [detail] [long]</td>
<td>Shows TCP Intercept statistics. The display includes the top 10 protected servers under attack. You can include the following keywords:</td>
</tr>
<tr>
<td>- all shows the history data of all the traced servers.</td>
<td></td>
</tr>
<tr>
<td>- detail shows history sampling data.</td>
<td></td>
</tr>
<tr>
<td>- long shows the statistical history in a long format, with the real and the translated IP addresses of the server.</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Threat detection statistics show both allowed and dropped traffic rates.

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger.
- The number of times the rates were exceeded (for dropped traffic statistics only).
- The total number of events over the fixed time periods.

The system computes the event counts 30 times over the average rate interval; in other words, the system checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20
minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the `show` command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the system calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

The following table explains the output for all commands with the exception of TCP Intercept views. See the TCP Intercept example for an explanation of that output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Name, ID</td>
<td>For Top reports, the column shows the name or number of the access control entry, the IP address of the host, or the name/ID number of the port or protocol. Entries are grouped by the fixed rate intervals and they are ranked within the time period, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so fewer than 10 items might be shown for a given interval. For host and port-protocol, the groupings are by sent and received bytes and packets per fixed interval.</td>
</tr>
<tr>
<td>Average(eps)</td>
<td>Shows the average rate in events/sec over each time period. The system stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the show command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the system calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.</td>
</tr>
<tr>
<td>Current(eps)</td>
<td>Shows the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00.</td>
</tr>
<tr>
<td>Trigger</td>
<td>Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total events</td>
<td>Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the system calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.</td>
</tr>
<tr>
<td>Entry heading</td>
<td>The statistics are grouped by fixed interval under a heading. The heading can include the information explained in the following rows. In general, the entry heading starts with the following:</td>
</tr>
<tr>
<td></td>
<td>• Host, with the host IP address.</td>
</tr>
<tr>
<td></td>
<td>• The port number/name. For example, 80/HTTP.</td>
</tr>
<tr>
<td></td>
<td>• The protocol number or name. For example, ICMP.</td>
</tr>
<tr>
<td></td>
<td>• For top reports, the fixed interval and statistics type. For access-list, the heading indicates this is for ACL hits.</td>
</tr>
<tr>
<td>tot-ses</td>
<td>Shows the total number of sessions for this host, port, or protocol since it was added to the database.</td>
</tr>
<tr>
<td>act-ses</td>
<td>Shows the total number of active sessions that the host, port, or protocol is currently involved in.</td>
</tr>
<tr>
<td>fw-drop</td>
<td>Shows the number of firewall drops. Firewall drops is a combined rate that includes all firewall-related packet drops tracked in basic threat detection, including access list denials, bad packets, exceeded connection limits, DoS attack packets, suspicious ICMP packets, TCP SYN attack packets, and UDP session with no return data attack packets. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.</td>
</tr>
<tr>
<td></td>
<td>(Host only.)</td>
</tr>
<tr>
<td>insp-drop</td>
<td>Shows the number of packets dropped because they failed application inspection.</td>
</tr>
<tr>
<td></td>
<td>(Host only.)</td>
</tr>
<tr>
<td>null-ses</td>
<td>Shows the number of null sessions, which are TCP SYN sessions that did not complete within the 30-second timeout, and UDP sessions that did not have any data sent by its server 3 seconds after the session starts.</td>
</tr>
<tr>
<td></td>
<td>(Host only.)</td>
</tr>
<tr>
<td>bad-acc</td>
<td>Shows the number of bad access attempts to host ports that are in a closed state. When a port is determined to be in a null session (see above), the port state of the host is set to HOST_PORT_CLOSE. Any client accessing the port of the host is immediately classified as a bad access without the need to wait for a timeout.</td>
</tr>
<tr>
<td></td>
<td>(Host only.)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>20-min, 1-hour, 8-hour, and 24-hour</td>
<td>Shows statistics for these fixed rate intervals.</td>
</tr>
<tr>
<td></td>
<td>• Sent byte, sent pkts—Shows the number of successful bytes or packets sent from the host, port, or protocol.</td>
</tr>
<tr>
<td></td>
<td>• Sent drop—Shows the number of packets sent from the host, port, or protocol that were dropped because they were part of a scanning attack.</td>
</tr>
<tr>
<td></td>
<td>• Recv byte, pkts—Shows the number of successful bytes or packets received by the host, port, or protocol.</td>
</tr>
<tr>
<td></td>
<td>• Recv drop—Shows the number of packets received by the host, port, or protocol that were dropped because they were part of a scanning attack.</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the `show threat-detection statistics host` command:

```
> show threat-detection statistics host

<table>
<thead>
<tr>
<th>Average(eps)</th>
<th>Current(eps)</th>
<th>Trigger</th>
<th>Total events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-hour Sent byte: 2938 0 0 10580308</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-hour Sent byte: 367 0 0 10580308</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24-hour Sent byte: 122 0 0 10580308</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-hour Sent pkts: 28 0 0 104043</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-hour Sent pkts: 3 0 0 104043</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24-hour Sent pkts: 1 0 0 104043</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20-min Sent drop: 9 0 1 10851</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-hour Sent drop: 3 0 1 10851</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-hour Recv byte: 2697 0 0 9712670</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-hour Recv byte: 337 0 0 9712670</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24-hour Recv byte: 112 0 0 9712670</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-hour Recv pkts: 29 0 0 104846</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-hour Recv pkts: 3 0 0 104846</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24-hour Recv pkts: 1 0 0 104846</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20-min Recv drop: 42 0 3 50567</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-hour Recv drop: 14 0 1 50567</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0 |
| 1-hour Sent byte: 0 0 0 614 |
| 8-hour Sent byte: 0 0 0 614 |
| 24-hour Sent byte: 0 0 0 614 |
| 1-hour Sent pkts: 0 0 0 6 |
| 8-hour Sent pkts: 0 0 0 6 |
| 24-hour Sent pkts: 0 0 0 6 |
| 20-min Sent drop: 0 0 0 4 |
| 1-hour Sent drop: 0 0 0 4 |
| 1-hour Recv byte: 0 0 0 706 |
| 8-hour Recv byte: 0 0 0 706 |
| 24-hour Recv byte: 0 0 0 706 |
| 1-hour Recv pkts: 0 0 0 7 |
```

The following is sample output from the `show threat-detection statistics port` command:

```
> show threat-detection statistics port
```
The following is sample output from the `show threat-detection statistics protocol` command:

```
> show threat-detection statistics protocol

Average(eps) Current(eps) Trigger Total events
80/HTTP: tot-ses:310971 act-ses:22571
1-hour Sent byte: 2939 0 0 10580922
8-hour Sent byte: 367 22043 0 10580922
24-hour Sent byte: 122 7347 0 10580922
1-hour Sent pkts: 28 0 0 104049
8-hour Sent pkts: 3 216 0 104049
24-hour Sent pkts: 1 72 0 104049
20-min Sent drop: 9 0 2 10855
1-hour Sent drop: 3 0 2 10855
1-hour Recv byte: 2698 0 0 9713376
8-hour Recv byte: 112 6745 0 9713376
24-hour Recv byte: 122 7347 0 9713376
1-hour Recv pkts: 29 0 0 104049
8-hour Recv pkts: 29 0 0 104853
24-hour Recv pkts: 29 0 0 104853
20-min Recv drop: 24 0 2 29134
1-hour Recv drop: 8 0 2 29134
```

The following is sample output from the `show threat-detection statistics top access-list` command:

```
> show threat-detection statistics top access-list

Top Average(eps) Current(eps) Trigger Total events
1-hour ACL hits:
100/3[0] 173 0 0 623488
200/2[1] 43 0 0 156786
100/1[2] 43 0 0 156786
8-hour ACL hits:
100/3[0] 21 1298 0 623488
200/2[1] 5 326 0 156786
100/1[2] 5 326 0 156786
```

The following is sample output from the `show threat-detection statistics top port-protocol` command:

```
> show threat-detection statistics top port-protocol

Top Name Id Average(eps) Current(eps) Trigger Total events
1-hour Recv byte:
1 gopher 70 71 0 0 32345678
2 btp-clnt/dhcp 68 68 0 0 27345678
3 gopher 69 65 0 0 24345678
4 Protocol-96 * 96 63 0 0 22345678
5 Port-7314 62 62 0 0 19345678
6 BitTorrent/trc 69 61 0 0 16345678
7 Port-8191-65535 55 55 0 0 12345678
8 SMTP 366 34 0 0 32345678
```

Cisco Firepower Threat Defense Command Reference

890
The following is sample output from the `show threat-detection statistics top host` command:

```
> show threat-detection statistics top host

<table>
<thead>
<tr>
<th></th>
<th>Top Average(eps)</th>
<th>Current(eps)</th>
<th>Trigger</th>
<th>Total events</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-hour</td>
<td>10.0.0.1[0]</td>
<td>2938</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sent byte:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sent pkts:</td>
<td>10.0.0.1[0]</td>
<td>28</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>20-min</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sent drop:</td>
<td>10.0.0.1[0]</td>
<td>9</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1-hour</td>
<td>10.0.0.1[0]</td>
<td>2697</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Recv byte:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recv pkts:</td>
<td>10.0.0.1[0]</td>
<td>29</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1-hour</td>
<td>10.0.0.1[0]</td>
<td>23</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sent pkts:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20-min</td>
<td>10.0.0.1[0]</td>
<td>42</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Sent drop:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-hour</td>
<td>10.0.0.1[0]</td>
<td>367</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sent byte:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sent pkts:</td>
<td>10.0.0.1[0]</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1-hour</td>
<td>10.0.0.1[0]</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Recv drop:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-hour</td>
<td>10.0.0.1[0]</td>
<td>337</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Recv byte:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recv pkts:</td>
<td>10.0.0.1[0]</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1-hour</td>
<td>10.0.0.1[0]</td>
<td>14</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Recv drop:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24-hour</td>
<td>10.0.0.1[0]</td>
<td>122</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sent byte:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sent pkts:</td>
<td>10.0.0.1[0]</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24-hour</td>
<td>10.0.0.1[0]</td>
<td>112</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Recv byte:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recv pkts:</td>
<td>10.0.0.1[0]</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

The following is sample output from the `show threat-detection statistics top tcp-intercept` command:

```
> show threat-detection statistics top tcp-intercept

Top 10 protected servers under attack (sorted by average rate)
```
The following table explains the TCP Intercept output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring window size</td>
<td>Shows the period of time over which the system samples data for statistics. The default is 30 minutes. You can change this setting using the command <code>threat-detection statistics tcp-intercept rate-interval</code> using FlexConfig. The system samples data 30 times during this interval.</td>
</tr>
<tr>
<td>Sampling interval</td>
<td>Shows the interval between samples. This value is always the rate interval divided by 30.</td>
</tr>
<tr>
<td>Rank</td>
<td>Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.</td>
</tr>
<tr>
<td>Server IP:Port</td>
<td>Shows the server IP address and the port on which it is being attacked.</td>
</tr>
<tr>
<td>Interface</td>
<td>Shows the interface through which the server is being attacked.</td>
</tr>
<tr>
<td>Ave Rate</td>
<td>Shows the average rate of attack, in attacks per second over the sampling period.</td>
</tr>
<tr>
<td>Cur Rate</td>
<td>Shows the current attack rate, in attacks per second.</td>
</tr>
<tr>
<td>Total</td>
<td>Shows the total number of attacks.</td>
</tr>
<tr>
<td>Source IP</td>
<td>Shows the attacker IP address.</td>
</tr>
<tr>
<td>Last Attack Time</td>
<td>Shows when the last attack occurred.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show threat-detection statistics top tcp-intercept long` command with the real server IP address in parentheses:

```
> show threat-detection statistics top tcp-intercept long

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack Time)>
----------------------------------------------------------------------------------
1  10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 53911 10.0.0.201 (0 secs ago)
2  10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 53911 10.0.0.201 (0 secs ago)
3  10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 53911 10.0.0.201 (0 secs ago)
4  10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 53911 10.0.0.201 (0 secs ago)
```
The following is sample output from the `show threat-detection statistics top tcp-intercept detail` command, which shows the sampling data. The sampling data is the number of attacks for each of the 30 sampling periods.

```
> show threat-detection statistics top tcp-intercept detail
Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins  Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack Time)>
----------------------------------------------------------------------------------
1  192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
Sampling History (30 Samplings):
  95348 95337 95341 95339 95338 95342
  95337 95348 95342 95338 95339 95340
  95339 95337 95342 95348 95338 95342
  95348 95339 95340 95339 95349 95343
  95337 95339 95342 95338 95342
  95338 95339 95340 95339 95340 95340
  96351 96351 96119 95339 95349 95341
  95338 95337 95342 95338 95342
  95337 95339 95342 95338 95342
  95338 95337 95342 95338 95342
  95338 95337 95342 95338 95342
  95338 95337 95342 95338 95342
  95338 95337 95342 95338 95342
  95338 95337 95342 95338 95342
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear threat-detection statistics</td>
<td>Clears threat detection statistics.</td>
</tr>
<tr>
<td>show running-config all threat-detection</td>
<td>Shows the threat detection configuration, including the default rate settings if you did not configure them individually.</td>
</tr>
</tbody>
</table>
show time

To display UTC and local time and date for the device, use the `show time` command.

```
show time
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show time` command.

```
> show time
UTC - Wed Aug 3 17:04:06 UTC 2016
Localtime - Wed Aug 03 13:04:06 EDT 2016
```
show time-range

To display the configuration of all time range objects, use the `show time-range` command

```
show time-range [name]
```

### Syntax Description

| name | (Optional) Shows information for this time range object only. |

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to display the configuration of the time range objects. In this example, there is one object, which is named work-hours. Inactive means that the object is not being used.

```
> show time-range

time-range entry: work-hours (inactive)
  periodic weekdays 9:00 to 17:00
```
show tls-proxy

To display TLS proxy and session information for encrypted inspections, use the `show tls-proxy` command.

```
show tls-proxy [tls_name | session [host host_address | detail [cert-dump] | count | statistics ]]
```

**Syntax Description**

- **count**: Shows only the session counters.
- **detail [cert-dump]**: Shows detailed TLS proxy information including the cipher for each SSL leg and the LDC. Add the `cert-dump` keyword to get a hexadecimal dump of the local dynamic certificate (LDC).
  
  You can also use these keywords with the `host` option.
- **host host_address**: Specifies the IPv4 or IPv6 address of a particular host to show the associated sessions associated.
- **session**: Shows active TLS proxy sessions.
- **statistics**: Shows statistics for monitoring and managing TLS sessions.
- **tls_name**: The name of the TLS proxy to show.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The TLS proxies you can view with this command are those configured for encrypted application inspections only. They apply to the SIP, SCCP (Skinny), or Diameter inspections. These TLS proxies are not related to the SSL Decryption or VPN policies.

**Examples**

The following is sample output from the `show tls-proxy` command:

```
> show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
  Server proxy:
    Trust-point: local_ccm
  Client proxy:
    Local dynamic certificate issuer: ldc_signer
    Local dynamic certificate key-pair: phone_common
    Cipher-suite <unconfigured>
  Run-time proxies:
    Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
      Active sess 1, most sess 4, byte 3244
```

The following is sample output from the `show tls-proxy session` command:

```
> show tls-proxy session
```

The following is sample output from the `show tls-proxy session detail` command:

```bash
> show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte 1831704
   Client: State SSLOK Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1
   Server: State SSLOK Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
   Status: Available
   Certificate Serial Number: 29
   Certificate Usage: General Purpose
   Public Key Type: RSA (1024 bits)
   Issuer Name:
      cn=TLS-Proxy-Signer
   Subject Name:
      cn=SEP0002B9EB0AAD
      o=Cisco Systems Inc
      c=US
   Validity Date:
      start date: 00:47:12 PDT Feb 27 2007
      end date: 00:47:12 PDT Feb 27 2008
   Associated Trustpoints:
```

The following is sample output from the `show tls-proxy session statistics` command:

```bash
> show tls-proxy session statistics
TLS Proxy Sessions (Established: 600)
   Mobility: 0
Per-Session Licensed TLS Proxy Sessions
   (Established: 222, License Limit: 3000)
      SIP: 2
      SCCP: 20
      DIAMETER: 200
Total TLS Proxy Sessions
   Established: 822
   Platform Limit: 1000
```
show track

To display information about object tracked by the security-level agreement (SLA) tracking process, use the `show track` command.

`show track [track-id]`

**Syntax Description**

| track-id | A tracking entry object ID number, from 1 to 500. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show track` command:

```
> show track
Track 5
  Response Time Reporter 124 reachability
  Reachability is UP
  2 changes, last change 03:41:16
  Latest operation return code: OK
  Tracked by:
    STATIC-IP-ROUTING 0
```
**show traffic**

To display interface transmit and receive activity, use the `show traffic` command.

```plaintext
show traffic
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show traffic` command lists the number of packets and bytes moving through each interface since the last `show traffic` command was entered or since the device came online. The number of seconds is the duration the device has been online since the last reboot, unless the `clear traffic` command was entered since the last reboot. If this is the case, then the number of seconds is the duration since that command was entered.

The statistics are first shown based on interface name. After the named interfaces, statistics are shown based on the physical interface. The interfaces can include hidden virtual interfaces that are used by the system for internal communications.

**Examples**

The following is an abbreviated sample output from the `show traffic` command, showing the statistics for a single interface. Each interface shows the same statistics.

```plaintext
> show traffic
... diagnostic:
   received (in 102.080 secs):
     2048 packets  204295 bytes
     20 pkts/sec  2001 bytes/sec
   transmitted (in 102.080 secs):
     2048 packets  204056 bytes
     20 pkts/sec  1998 bytes/sec
   1 minute input rate 122880 pkts/sec, 5775360 bytes/sec
   1 minute output rate 122887 pkts/sec, 5775389 bytes/sec
   1 minute drop rate, 3 pkts/sec
   5 minute input rate 118347 pkts/sec, 5562309 bytes/sec
   5 minute output rate 119221 pkts/sec, 5603387 bytes/sec
   5 minute drop rate, 11 pkts/sec
... 
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear traffic</td>
<td>Resets the counters for transmit and receive activity.</td>
</tr>
</tbody>
</table>
show user

To show the user accounts for accessing the command line interface (CLI) on the device, use the `show user` command.

```
show user [username1 [username2] [...]]
```

### Syntax Description

- `username1 [username2]` (Optional.) One or more space-separated user names. If you do not specify any names, all users are shown.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The following information is shown for each user. Create user accounts with the `configure user add` command.

- **Login**—The login name.
- **UID**—The numeric user ID.
- **Auth**—How the user is authenticated, either Local or Remote (through a directory server).
- **Access**—The user's privilege level, Basic or Config. Use the `configure user access` command to change this setting.
- **Enabled**—Whether the user is active, Enabled or Disabled. Use the `configure user enable/disable` commands to change this setting.
- **Reset**—Whether the user must change the account password at the next login, Yes or No. Use the `configure user forcereset` command to change this setting.
- **Exp**—The number of days until the user's password must be changed. Never indicates that the password does not expire. Use the `configure user aging` command to change this setting.
- **Warn**—The number of days a user is given to change their password before it expires. N/A indicates that warnings are not applicable. Use the `configure user aging` command to change this setting.
- **Str**—Whether the user's password must meet strength checking criteria, Dis (disabled) or Ena (enabled). Configure this option with the `configure user strengthcheck` command.
- **Lock**—Whether the user's account has been locked due to too many login failures, Yes or No. Use the `configure user unlock` command to unlock a user account.
- **Max**—The maximum number of failed logins before the user's account is locked. N/A indicates the account can never be locked. Use the `configure user maxfailedlogins` command to change this setting.

### Examples

The following example shows how to display the users defined for CLI access.

```
> show user
Login   UID  Auth Access   Enabled Reset   Exp Warn   Str   Lock Max
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure user add</td>
<td>Add a user account for CLI access.</td>
</tr>
</tbody>
</table>
show version

To display the hardware model, software version, UUID, intrusion rule update version, and VDB version, use the `show version` command.

`show version` [detail | system]

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td><code>show version</code> and <code>show version detail</code> display the same information.</td>
</tr>
<tr>
<td>system</td>
<td>This keyword appends additional system information to the information displayed by <code>show version</code>.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show version` command and the `show version detail` command display the same basic system information. The `show version system` command displays this information plus additional system information such as operating time since the last reboot and more specific hardware information.

**Examples**

The following example shows the basic `show version` output.

```bash
> show version
--------------[ example-sfr.example.com ]--------------
Model : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build 226)
UUID  : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version : 2016-03-28-001-vrt
VDB version : 270
--------------
```

The following sample output from the `show version system` command appends the same output as the `show version` command with additional information.

```bash
> show version system
--------------[ example-sfr.example.com ]--------------
Model : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build 226)
UUID  : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version : 2016-03-28-001-vrt
VDB version : 270
--------------
Cisco Adaptive Security Appliance Software Version 9.6(1)72
Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"
firepower up 36 days 21 hours
Hardware: ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
```
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device: Cisco ASA Crypto on-board accelerator (revision 0x1)

Number of accelerators: 1

1: Ext: GigabitEthernet1/1 : address is e865.49b8.97f2, irq 255
2: Ext: GigabitEthernet1/2 : address is e865.49b8.97f3, irq 255
3: Ext: GigabitEthernet1/3 : address is e865.49b8.97f4, irq 255
4: Ext: GigabitEthernet1/4 : address is e865.49b8.97f5, irq 255
5: Ext: GigabitEthernet1/5 : address is e865.49b8.97f6, irq 255
6: Ext: GigabitEthernet1/6 : address is e865.49b8.97f7, irq 255
7: Ext: GigabitEthernet1/7 : address is e865.49b8.97f8, irq 255
8: Ext: GigabitEthernet1/8 : address is e865.49b8.97f9, irq 255
9: Int: Internal-Data1/1 : address is e865.49b8.97f1, irq 255
10: Int: Internal-Data1/2 : address is 0000.0001.0002, irq 0
11: Int: Internal-Control1/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3 : address is 0000.0001.0003, irq 0
13: Ext: Management1/1 : address is e865.49b8.97f1, irq 0
14: Int: Internal-Data1/4 : address is 0000.0100.0001, irq 0

Serial Number: JAD192100RG
Configuration register is 0x1
Image type: Release
Key Version: A
Configuration last modified by enable_1 at 12:44:37.849 UTC Mon Jul 25 2016
show vlan

To display all VLANs configured on the Firepower Threat Defense device, use the `show vlan` command.

```
show vlan  [mapping  [primary_id]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mapping</code></td>
<td>(Optional) Shows the secondary VLANs mapped to the primary VLAN.</td>
</tr>
<tr>
<td><code>primary_id</code></td>
<td>(Optional) Shows secondary VLANs for a specific primary VLAN.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the configured VLANs:

```
> show vlan
10-11,30,40,300
```

The following example displays the secondary VLANs that are mapped to each primary VLAN:

```
> show vlan mapping

<table>
<thead>
<tr>
<th>Interface</th>
<th>Secondary VLAN ID</th>
<th>Mapped VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1.100</td>
<td>200</td>
<td>300</td>
</tr>
<tr>
<td>0/1.100</td>
<td>201</td>
<td>300</td>
</tr>
<tr>
<td>0/2.500</td>
<td>400</td>
<td>200</td>
</tr>
</tbody>
</table>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear interface</td>
<td>Clears counters for the <code>show interface</code> command.</td>
</tr>
<tr>
<td>show interface</td>
<td>Displays the runtime status and statistics of interfaces.</td>
</tr>
</tbody>
</table>
show vm

To display virtual platform information on the Firepower Threat Defense Virtual device, use the `show vm` command.

**Example**

The following example shows how to display information on VMware:

```
> show vm

Virtual Platform Resource Status
-------------------------------
Number of vCPUs : 4
Processor Memory : 8192 MB
Hypervisor : VMware
```
show vpdn

To show the status of virtual private dial-up network (VPDN) connections such as PPPoE or L2TP, use the `show vpdn` command.

```
show vpdn { group name | pppinterface id number | session { l2tp | pppoe } id number { packets | state | window } | tunnel { l2tp | pppoe } id number { packets | state | summary | transport } | username name }
```

### Syntax Description

- **group name**: Shows the VPDN group configuration.
- **id number**: (Optional) Shows information about the VPDN session with the specified ID.
- **l2tp**: (Optional) Shows session or tunnel information about L2TP.
- **packets**: Shows session or tunnel packet information.
- **pppinterface**: Shows PPP interface information.
- **pppoe**: (Optional) Shows session or tunnel information about PPPoE.
- **session**: Shows session information.
- **state**: Shows session or tunnel state information.
- **summary**: Shows the tunnel summary.
- **transport**: Shows tunnel transport information.
- **tunnel**: Shows tunnel information.
- **username name**: Shows user information.
- **window**: Shows session window information.

### Command History

- **Release**  | **Modification**  
- **6.1**    | This command was introduced.

### Usage Guidelines

Use this command to troubleshoot the VPDN PPPoE or L2TP connections.

### Examples

The following is sample output from the `show vpdn session` command:

```
> show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
```
PPP interface id is 1
6 packets sent, 6 received, 84 bytes sent, 0 received

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

```
> show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
  time since change 65901 secs
  Remote Internet Address 10.0.0.1
  Local Internet Address 199.99.99.3
```
show vpn load-balancing

Do not use this command. It relates to a feature not supported by Firepower Threat Defense.
show vpn-sessiondb

To display information about VPN sessions, use one of the `show vpn-sessiondb` commands.

```
show vpn-sessiondb [detail] [full] {anyconnect | l2l | ra-ikev1-ipsec | ra-ikev2-ipsec} [filter criteria] [sort criteria]
show vpn-sessiondb failover
show vpn-sessiondb ospfv3 [filter ipaddress IP_address] [sort ipaddress]
```

### Syntax Description

- **anyconnect**
  
  Displays AnyConnect VPN client sessions.

- **detail**
  
  (Optional) Displays extended details about a session. For example, using the detail option for an IPsec session displays additional details such as the IKE hashing algorithm, authentication mode, and rekey interval.

  If you choose detail, and the full option, the Firepower Threat Defense device displays the detailed output in a machine-readable format.

- **failover**
  
  Displays the session information for the failover IPsec tunnels.

- **filter filter_criteria**
  
  (Optional) Filters the output to according to the filter option you specify. For a list of options, see the “Usage Guidelines” section.

- **full**
  
  (Optional) Displays streamed, untruncated output. Output is delineated by | characters and a || string between records.

- **index indexnumber**
  
  Displays a single session by index number. Specify the index number for the session, which ranges from 1 - 65535.

- **l2l**
  
  Displays VPN LAN-to-LAN session information.

- **ospfv3**
  
  Displays OSPFv3 session information.

- **ra-ikev1-ipsec**
  
  Displays IPsec IKEv1 sessions.

- **ra-ikev2-ipsec**
  
  Displays details for IKEv2 remote access client connections.

- **sort sort_criteria**
  
  (Optional) Sorts the output according to the sort option you specify. For a list of options, see the “Usage Guidelines” section.

### Command History

- **Release**
  
<table>
<thead>
<tr>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
</tr>
<tr>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You can use the following options to filter and to sort the session display. The values you can filter and sort on differ based on the session types you are listing.
<table>
<thead>
<tr>
<th>Filter/Sort Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>filter a-ipaddress</strong></td>
<td>Filters the output to display information for the specified assigned IP address or addresses only.                                        Use with: anyconnect, ra-ikev2-ipsec</td>
</tr>
<tr>
<td><strong>IP_address</strong></td>
<td></td>
</tr>
<tr>
<td><strong>sort a-ipaddress</strong></td>
<td>Sorts the display by assigned IP addresses.                                                                                                     Use with: anyconnect, ra-ikev2-ipsec</td>
</tr>
<tr>
<td><strong>filter a-ipversion</strong></td>
<td>Filters the output to show only sessions assigned IPv4 or IPv6 addresses.                                                                 Use with: anyconnect, ra-ikev2-ipsec</td>
</tr>
<tr>
<td>**{v4</td>
<td>v6}**</td>
</tr>
<tr>
<td><strong>filter encryption</strong></td>
<td>Filters the output to display information for sessions using the specified encryption algorithm only. Use ? to see the available methods. Use with: anyconnect, 12l, ra-ikev2-ipsec</td>
</tr>
<tr>
<td><strong>encryption_algorithm</strong></td>
<td></td>
</tr>
<tr>
<td><strong>sort encryption</strong></td>
<td>Sorts the output by the encryption algorithm used in the session.                                                                 Use with: anyconnect, 12l, ra-ikev2-ipsec</td>
</tr>
<tr>
<td><strong>filter inactive</strong></td>
<td>Filters by inactive sessions, which are sessions that have gone idle and have possibly lost connectivity (due to hibernation, mobile device disconnection, and so on). The number of inactive sessions increases when TCP keepalives are sent from the Firepower Threat Defense device without a response from the AnyConnect client. Each session is time stamped with the SSL tunnel drop time. If the session is actively passing traffic over the SSL tunnel, 00:00m:00s is displayed. Use with: anyconnect</td>
</tr>
<tr>
<td><strong>sort inactivity</strong></td>
<td>Sorts by inactive sessions.                                                                                                                      Use with: anyconnect</td>
</tr>
<tr>
<td><strong>filter ipaddress</strong></td>
<td>Filters the output to display information for the specified inside IP address or addresses only.                                                        Use with: 12l, ospfv3</td>
</tr>
<tr>
<td><strong>IP_address</strong></td>
<td></td>
</tr>
<tr>
<td><strong>sort ipaddress</strong></td>
<td>Sorts the display by inside IP addresses.                                                                                                        Use with: 12l, ospfv3</td>
</tr>
<tr>
<td><strong>filter ipversion</strong></td>
<td>Filters the output to show only sessions originating from endpoints with IPv4 or IPv6 addresses.                                                        Use with: 12l</td>
</tr>
<tr>
<td>**{v4</td>
<td>v6}**</td>
</tr>
</tbody>
</table>
**Filter/Sort Option** | **Description**
--- | ---
**filter name** *username* | Filters the output to display sessions for the specified username. Use with: `anyconnect, l2l, ra-ikev2-ipsec`
**sort name** | Sorts the display by usernames in alphabetical order. Use with: `anyconnect, l2l, ra-ikev2-ipsec`
**filter p-ipaddress** *IP_address* | Filters the output to display information for the specified public outside IP address or addresses only. Use with: `anyconnect, ra-ikev2-ipsec`
**sort p-ipaddress** | Sorts the display by public outside IP addresses. Use with: `anyconnect, ra-ikev2-ipsec`
**filter p-ipversion** {v4 | v6} | Filters the output to show only sessions originating from endpoints with public IPv4 or IPv6 addresses. Use with: `anyconnect, ra-ikev2-ipsec`
**filter protocol** *name* | Filters the output to display information for sessions using the specified protocol only. Use ? to see the available protocols. Use with: `anyconnect, l2l, ra-ikev2-ipsec`
**sort protocol** | Sorts the display by protocol. Use with: `anyconnect, l2l, ra-ikev2-ipsec`

The following table explains the fields you might see in the output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Mode</td>
<td>Protocol or mode used to authenticate this session.</td>
</tr>
<tr>
<td>Bytes Rx</td>
<td>Total number of bytes received from the remote peer or client by the system.</td>
</tr>
<tr>
<td>Bytes Tx</td>
<td>Number of bytes transmitted to the remote peer or client by the system.</td>
</tr>
<tr>
<td>Client Type</td>
<td>Client software running on the remote peer, if available.</td>
</tr>
<tr>
<td>Client Ver</td>
<td>Version of the client software running on the remote peer.</td>
</tr>
<tr>
<td>Connection</td>
<td>Name of the connection or the private IP address.</td>
</tr>
<tr>
<td>D/H Group</td>
<td>Diffie-Hellman Group. The algorithm and key size used to generate IPsec SA encryption keys.</td>
</tr>
<tr>
<td>Duration</td>
<td>Elapsed time (HH:MM:SS) between the session login time and the last screen refresh.</td>
</tr>
<tr>
<td>EAPoUDP Session Age</td>
<td>Number of seconds since the last successful posture validation.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Mode used to apply IPsec ESP (Encapsulation Security Payload protocol) encryption and authentication (that is, the part of the original IP packet that has ESP applied).</td>
</tr>
<tr>
<td>Encryption</td>
<td>Data encryption algorithm this session is using, if any.</td>
</tr>
<tr>
<td>EoU Age (T)</td>
<td>EAPoUDP Session Age. Number of seconds since the last successful posture validation.</td>
</tr>
<tr>
<td>Filter Name</td>
<td>Username specified to restrict the display of session information.</td>
</tr>
<tr>
<td>Hashing</td>
<td>Algorithm used to create a hash of the packet, which is used for IPsec data authentication.</td>
</tr>
<tr>
<td>Hold Left (T)</td>
<td>Hold-Off Time Remaining. 0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.</td>
</tr>
<tr>
<td>Hold-Off Time Remaining</td>
<td>0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.</td>
</tr>
<tr>
<td>IKE Neg Mode</td>
<td>IKE (IPsec Phase 1) mode for exchanging key information and setting up SAs: Aggressive or Main.</td>
</tr>
<tr>
<td>IKE Sessions</td>
<td>Number of IKE (IPsec Phase 1) sessions; usually 1. These sessions establish the tunnel for IPsec traffic.</td>
</tr>
<tr>
<td>Index</td>
<td>Unique identifier for this record.</td>
</tr>
<tr>
<td>IP Addr</td>
<td>Private IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address. It lets the client appear to be a host on the private network.</td>
</tr>
<tr>
<td>IPsec Sessions</td>
<td>Number of IPsec (Phase 2) sessions, which are data traffic sessions through the tunnel. Each IPsec remote-access session can have two IPsec sessions: one consisting of the tunnel endpoints, and one consisting of the private networks reachable through the tunnel.</td>
</tr>
<tr>
<td>License Information</td>
<td>Shows information about the shared SSL VPN license.</td>
</tr>
<tr>
<td>Local IP Addr</td>
<td>IP address assigned to the local endpoint of the tunnel (that is the interface on the system).</td>
</tr>
<tr>
<td>Login Time</td>
<td>Date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.</td>
</tr>
</tbody>
</table>
State of Network Admission Control Posture Validation. It can be one of the following:

- Accepted—The ACS successfully validated the posture of the remote host.
- Rejected—The ACS could not successfully validate the posture of the remote host.
- Exempted—The remote host is exempt from posture validation according to the Posture Validation Exception list configured on the Firepower Threat Defense device.
- Non-Responsive—The remote host did not respond to the EAPoUDP Hello message.
- Hold-off—The Firepower Threat Defense device lost EAPoUDP communication with the remote host after successful posture validation.
- N/A—NAC is disabled for the remote host according to the VPN NAC group policy.
- Unknown—Posture validation is in progress.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAC Result</td>
<td>State of Network Admission Control Posture Validation. It can be one of the following:</td>
</tr>
<tr>
<td>NAC Sessions</td>
<td>Number of Network Admission Control (EAPoUDP) sessions.</td>
</tr>
<tr>
<td>Packets Rx</td>
<td>Number of packets received from the remote peer by the system.</td>
</tr>
<tr>
<td>Packets Tx</td>
<td>Number of packets transmitted to the remote peer by the system.</td>
</tr>
<tr>
<td>PFS Group</td>
<td>Perfect Forward Secrecy group number.</td>
</tr>
<tr>
<td>Posture Token</td>
<td>Informational text string configurable on the Access Control Server. The ACS downloads the posture token to the system for informational purposes to aid in system monitoring, reporting, debugging, and logging. A typical posture token is Healthy, Checkup, Quarantine, Infected, or Unknown.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol the session is using.</td>
</tr>
<tr>
<td>Public IP</td>
<td>Publicly routable IP address assigned to the client.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the system. The Redirect URL is an optional part of the access policy payload. The system redirects all HTTP (port 80) and HTTPS (port 443) requests for the remote host to the Redirect URL if it is present. If the access policy does not contain a Redirect URL, the Firepower Threat Defense device does not redirect HTTP and HTTPS requests from the remote host. Redirect URLs remain in force until either the IPsec session ends or until posture revalidation, for which the ACS downloads a new access policy that can contain a different redirect URL or no redirect URL.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rekey Int (T or D)</td>
<td>Lifetime of the IPsec (IKE) SA encryption keys. The T value is the lifetime in duration, the D value is in data transmitted. Only the T value is shown for remote access VPN.</td>
</tr>
<tr>
<td>Rekey Left (T or D)</td>
<td>Lifetime remaining of the IPsec (IKE) SA encryption keys. The T value is the lifetime in duration, the D value is in data transmitted. Only the T value is shown for remote access VPN.</td>
</tr>
<tr>
<td>Rekey Time Interval</td>
<td>Lifetime of the IPsec (IKE) SA encryption keys.</td>
</tr>
<tr>
<td>Remote IP Addr</td>
<td>IP address assigned to the remote endpoint of the tunnel (that is the interface on the remote peer).</td>
</tr>
<tr>
<td>Reval Int (T)</td>
<td>Revalidation Time Interval. Interval in seconds required between each successful posture validation.</td>
</tr>
<tr>
<td>Reval Left (T)</td>
<td>Time Until Next Revalidation. 0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.</td>
</tr>
<tr>
<td>Revalidation Time Interval</td>
<td>Interval in seconds required between each successful posture validation.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Identifier for the session component (subsession). Each SA has its own identifier.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Type of session: LAN-to-LAN or Remote</td>
</tr>
<tr>
<td>SQ Int (T)</td>
<td>Status Query Time Interval. Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the system to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.</td>
</tr>
<tr>
<td>Status Query Time Interval</td>
<td>Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the system to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.</td>
</tr>
<tr>
<td>Time Until Next Revalidation</td>
<td>0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.</td>
</tr>
<tr>
<td>Tunnel Group</td>
<td>Name of the tunnel group referenced by this tunnel for attribute values.</td>
</tr>
<tr>
<td>UDP Dst Port or UDP Destination Port</td>
<td>Port number used by the remote peer for UDP.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
UDP Src Port or UDP Source Port | Port number used for UDP.
Username | User login name with which the session is established.
VLAN | Egress VLAN interface assigned to this session. The system forwards all traffic to that VLAN. One of the following elements specifies the value: Group policy or Inherited group policy

### Examples
The following is sample output from the `show vpn-sessiondb` command:

```
> show vpn-sessiondb
VPN Session Summary
---------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
---------------------------------------------------------------------------
AnyConnect Client : 1 : 12 : 3 : 0
SSL/TLS/DTLS : 1 : 12 : 3 : 0
Clientless VPN : 0 : 6 : 2
Browser : 0 : 6 : 2
---------------------------------------------------------------------------
Total Active and Inactive : 1 Total Cumulative : 18
Device Total VPN Capacity : 250
Device Load : 0%
---------------------------------------------------------------------------

Tunnels Summary
---------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
---------------------------------------------------------------------------
Clientless : 0 : 7 : 2
AnyConnect-Parent : 1 : 11 : 3
SSL-Tunnel : 1 : 12 : 3
DTLS-Tunnel : 1 : 12 : 3
---------------------------------------------------------------------------
Totals : 3 : 42
---------------------------------------------------------------------------
IPv6 Usage Summary
---------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
---------------------------------------------------------------------------
AnyConnect SSL/TLS/DTLS : : :
IPv6 Peer : 1 : 41 : 2
Tunneled IPv6 : 1 : 70 : 2
AnyConnect IKEv2 : : :
IPv6 Peer : 0 : 4 : 1
Clientless : : :
IPv6 Peer : 0 : 1 : 1
---------------------------------------------------------------------------
```
The following is sample output from the **show vpn-sessiondb detail** command:

```
> show vpn-sessiondb detail
VPN Session Summary
                      Active : Cumulative : Peak Concur : Inactive
----------------------------------------------
AnyConnect Client : 1 : 12 : 3 : 0
SSL/TLS/DTLS : 1 : 12 : 3 : 0
Clientless VPN : 0 : 6 : 2
Browser : 0 : 6 : 2

Total Active and Inactive : 1 Total Cumulative : 18
Device Total VPN Capacity : 250
Device Load : 0%

Tunnels Summary
                      Active : Cumulative : Peak Concurrent
----------------------------------------------
Clientless : 0 : 7 : 2
AnyConnect-Parent : 1 : 11 : 3
SSL-Tunnel : 1 : 12 : 3
DTLS-Tunnel : 1 : 12 : 3

Totals : 3 : 42
```

The following is sample output from the **show vpn-sessiondb detail l2l** command:

```
> show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed
Connection : 172.16.0.0
Index : 1
IP Addr : 172.16.0.0
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 240 Bytes Rx : 160
Login Time : 14:50:35 UTC Tue May 1 2017
Duration : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
Tunnel ID : 1.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86389 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
IPv6 Filter :

IPsec:
Tunnel ID : 1.2
Local Addr : 10.0.0.0/255.255.255.0
```
The following is sample output from the `show vpn-sessiondb detail index 1` command:

```
> show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username : user1
Index : 1
Assigned IP : 192.168.2.70 Public IP : 10.86.5.114
Protocol : IPsec Encryption : AES128
Hashing : SHA1
Bytes Tx : 0 Bytes Rx : 604533
Client Type : WinNT Client Ver : 4.6.00.0049
Tunnel Group : bxbvponlab
Login Time : 15:22:46 EDT Tue May 10 2005
Duration : 7h:02m:03s
Filter Name :
NAC Result : Accepted
Posture Token: Healthy
VM Result : Static
VLAN : 10

IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1

IKE:
Session ID : 1
UDP Src Port : 500 UDP Dst Port : 500
IKE Neg Mode : Aggressive Auth Mode : preSharedKeysXauth
Encryption : 3DES Hashing : MD5
Rekey Int (T): 86400 Seconds Rekey Left(T): 61078 Seconds
D/H Group : 2

IPsec:
Session ID : 2
Local Addr : 0.0.0.0
Remote Addr : 192.168.2.70
Encryption : AES128 Hashing : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 26531 Seconds
Bytes Tx : 0 Bytes Rx : 604533
Pkts Tx : 0 Pkts Rx : 8126

NAC:
Reval Int (T): 3000 Seconds Reval Left(T): 286 Seconds
SQ Int (T) : 600 Seconds EoU Age (T) : 2714 Seconds
Hold Left (T) : 0 Seconds Posture Token: Healthy
Redirect URL : www.cisco.com
```
The following is sample output from the `show vpn-sessiondb ospfv3` command:

```plaintext
> show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec

Connection:
Index : 1
IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none
Hashing : IPsec: (1)SHA1
Bytes Tx : 0
Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:13m:11s
```

The following is sample output from the `show vpn-sessiondb detail ospfv3` command:

```plaintext
> show vpn-sessiondb detail ospfv3

Session Type: OSPFv3 IPsec Detailed

Connection:
Index : 1
IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none
Hashing : IPsec: (1)SHA1
Bytes Tx : 0
Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:14m:28s
IPsec Tunnels: 1

IPsec:
Tunnel ID : 1.1
Local Addr : ::/0/89/0
Remote Addr : ::/0/89/0
Encryption : none
Hashing : SHA1
Encapsulation: Transport
Idle Time Out: 0 Minutes
Idle TO Left : 0 Minutes
Bytes Tx : 0
Bytes Rx : 0
Pkts Tx : 0
Pkts Rx : 0
NAC:
Reval Int (T): 0 Seconds
Reval Left(T): 0 Seconds
SQ Int (T): 0 Seconds
EoU Age(T): 105268 Seconds
Hold Left (T): 0 Seconds
Posture Token:
Redirect URL:
```

The following is sample output from the `show vpn-sessiondb detail anyconnect` command:

```plaintext
> show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : userab
Index : 2
Assigned IP : 65.2.1.100
Public IP : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)3DES
IPsecOverNatT: (1)3DES
AnyConnect-Parent: (1)none
Hashing : IKEv2: (1)SHA1
IPsecOverNatT: (1)SHA1
AnyConnect-Parent: (1)none
Bytes Tx : 0
Bytes Rx : 21248
Pkts Tx : 0
Pkts Rx : 238
Pkts Tx Drop : 0
Pkts Rx Drop : 0
```
The following is sample output from the `show vpn-sessiondb ra-ikev2-ipsec` command:

```bash
> show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Username : IKEV2TG Index : 1
Assigned IP : 95.0.225.200 Public IP : 85.0.224.12
Protocol : IKEv2 IPsec
License : AnyConnect Essentials
Encryption : IKEv2: (1)3DES IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
```
Bytes Tx : 0 Bytes Rx : 17844
Pkts Tx : 0 Pkts Rx : 230
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG Tunnel Group : IKEV2TG
Login Time : 11:39:54 UTC Tue May 6 2017
Duration : 0h:03m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none
IKEv2 Tunnels: 1
IPsec Tunnels: 1

The following is sample output from the `show vpn-sessiondb anyconnect` command:

```plaintext
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : user1  Index : 19576
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 15060  Bytes Rx : 20631
Group Policy : DfltGrpPolicy  Tunnel Group : Ad_group
Login Time : 09:24:53 UTC Fri Apr 7 2017
Duration : 0h:03m:20s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A  VLAN : none
Audt Sess ID : c0a8013804c7800058e75ae5
Security Grp : none  Tunnel Zone : 0
```

### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear vpn-sessiondb</td>
<td>Clears VPN session statistics.</td>
</tr>
<tr>
<td>clear vpn-sessiondb</td>
<td></td>
</tr>
<tr>
<td>statistics</td>
<td></td>
</tr>
<tr>
<td>show vpn-sessiondb</td>
<td>Displays VPN session encryption or protocol ratios.</td>
</tr>
<tr>
<td>ratio</td>
<td></td>
</tr>
<tr>
<td>show vpn-sessiondb</td>
<td>Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions.</td>
</tr>
<tr>
<td>summary</td>
<td></td>
</tr>
</tbody>
</table>
show vpn-sessiondb ratio

To display the ratio of current sessions as a percentage by protocol or encryption algorithm, use the `show vpn-sessiondb ratio` command.

```
show vpn-sessiondb ratio { encryption | protocol } [ filter  groupname ]
```

**Syntax Description**

- **encryption**
  - Displays the number of sessions and the percentage of sessions using each encryption method.

- **protocol**
  - Displays the number of sessions and the percentage of sessions using each VPN protocol.

- **filter  groupname**
  - (Optional.) Filters the output to include session ratios only for the tunnel group you specify.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display the ratio of sessions based on encryption.

```
> show vpn-sessiondb ratio encryption

Filter Group : All
Total Active Sessions: 5
Cumulative Sessions : 9
Encryption Tunnels Percent
none  0  0%   DES  0  0%   3DES  0  0%   RC4  0  0%   AES128  4  80%   AES192  1  20%   AES256  0  0%
AES-GCM-128  0  0%   AES-GCM-192  0  0%   AES-GCM-256  0  0%   AES-GMAC-128  0  0%   AES-GMAC-192  0  0%   AES-GMAC-256  0  0%
```

The following example shows how to display the ratio of sessions based on protocol.

```
> show vpn-sessiondb ratio protocol

Filter Group : All
Total Active Tunnels : 3
Cumulative Tunnels : 42
Protocol Tunnels Percent
```

Cisco Firepower Threat Defense Command Reference
### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show vpn-sessiondb</code></td>
<td>Displays information about VPN sessions.</td>
</tr>
<tr>
<td><code>show vpn-sessiondb summary</code></td>
<td>Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions.</td>
</tr>
</tbody>
</table>
show vpn-sessiondb summary

To display a summary of the number of active sessions, use the `show vpn-sessiondb summary` command.

```
show vpn-sessiondb summary
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The following table explains the fields in the Active Sessions and Session Information summaries:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent Limit</td>
<td>The maximum number of concurrently active sessions permitted on this system.</td>
</tr>
<tr>
<td>Cumulative Sessions</td>
<td>The number of sessions of all types since the system was last booted or reset.</td>
</tr>
<tr>
<td>LAN-to-LAN</td>
<td>The number of IPSec LAN-to-LAN sessions that are currently active.</td>
</tr>
<tr>
<td>Peak Concurrent</td>
<td>The highest number of sessions of all types that were concurrently active since the system was last booted or reset.</td>
</tr>
<tr>
<td>Percent Session Load</td>
<td>The percentage of the VPN session allocation in use. This value equals the Total Active Sessions divided by the maximum number of sessions available, displayed as a percentage.</td>
</tr>
<tr>
<td>Remote Access</td>
<td><code>ra-ikev1-ipsec</code>—The number of IKEv1 IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions that are currently active.</td>
</tr>
<tr>
<td>Total ActiveSessions</td>
<td>The number of sessions of all types that are currently active.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show vpn-sessiondb summary` command:

```
> show vpn-sessiondb summary
-------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
-------------------------------------------------------------------
OSPPFv3 : IPSec : 1 : 1
-------------------------------------------------------------------
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 10000
Device Load : 0%
-------------------------------------------------------------------
```

The following is sample output from the `show vpn-sessiondb summary` command for generic IKEv2 IPSec remote access sessions:
show vpn-sessiondb summary

VPN Session Summary

Active : Cumulative : Peak Concur : Inactive

Generic IKEv2 Remote Access : 1 : 1 : 1

Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 250
Device Load : 0%

Tunnels Summary

Active : Cumulative : Peak Concurrent

IKEv2 : 1 : 1 : 1
IPsec : 1 : 1 : 1

Totals : 2 : 2

Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vpn-sessiondb</td>
<td>Displays information about VPN sessions.</td>
</tr>
<tr>
<td>show vpn-sessiondb ratio</td>
<td>Displays VPN session encryption or protocol ratios.</td>
</tr>
</tbody>
</table>
# show wccp

To display global statistics related to Web Cache Communication Protocol (WCCP), use the `show wccp` command.

```plaintext
show wccp [web-cache | service_number] [buckets | detail | service | view | hash dest_addr source_addr dest_port source_port]
show wccp [interfaces [detail]]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>buckets</strong></td>
<td>(Optional) Displays service group bucket assignments.</td>
</tr>
<tr>
<td><strong>detail</strong></td>
<td>(Optional) Displays information about the router and all web caches.</td>
</tr>
<tr>
<td><strong>hash dest_addr</strong></td>
<td>Displays the WCCP hash for the specified connection:</td>
</tr>
<tr>
<td><strong>source_addr dest_port</strong></td>
<td>• <code>dest_addr</code> is the IP address of the destination host.</td>
</tr>
<tr>
<td></td>
<td>• <code>source_addr</code> is the IP address of the source host.</td>
</tr>
<tr>
<td></td>
<td>• <code>dest_port</code> is the port of the destination host.</td>
</tr>
<tr>
<td></td>
<td>• <code>source_port</code> is the port of the source host.</td>
</tr>
<tr>
<td><strong>interfaces [detail]</strong></td>
<td>(Optional) Displays the WCCP redirect interfaces. Include the detail keyword for the interface configuration.</td>
</tr>
<tr>
<td><strong>service</strong></td>
<td>(Optional) Displays service group definition information.</td>
</tr>
<tr>
<td><strong>service-number</strong></td>
<td>Identification number of the web-cache service group being controlled by the cache. The number can be from 0 to 254. For web caches using Cisco Cache Engines, the reverse proxy service is indicated by a value of 99.</td>
</tr>
<tr>
<td><strong>view</strong></td>
<td>(Optional) Displays whether other members of a particular service group have or have not been detected.</td>
</tr>
<tr>
<td><strong>web-cache</strong></td>
<td>Specifies statistics for the web-cache service.</td>
</tr>
</tbody>
</table>

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Examples

The following example shows how to display WCCP information:

```plaintext
> show wccp
Global WCCP information:
Router information:
  Router Identifier: -not yet determined-
  Protocol Version: 2.0
  Service Identifier: web-cache
```
### Number of Cache Engines: 0
### Number of routers: 0
### Total Packets Redirected: 0
### Redirect access-list: foo
### Total Connections Denied Redirect: 0
### Total Packets Unassigned: 0
### Group access-list: foobar
### Total Messages Denied to Group: 0
### Total Authentication failures: 0
### Total Bypassed Packets Received: 0

### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear wccp</td>
<td>Clears WCCP statistics.</td>
</tr>
</tbody>
</table>
**show webvpn**

To view information about remote access VPN, use the `show webvpn` command.

```
show webvpn   {anyconnect | debug-condition | group-alias [tunnel_group] | group-url [tunnel_group] | statistics}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>anyconnect</td>
<td>Displays information about the AnyConnect images that are available for download to client endpoints.</td>
</tr>
<tr>
<td>debug-condition</td>
<td>Displays the current debug conditions as set by the <code>debug webvpn condition</code> command.</td>
</tr>
<tr>
<td>group-alias [tunnel_group]</td>
<td>Displays the aliases for tunnel groups (connection profiles). You can optionally specify the name of a tunnel group to view information about that group only. Each group can have multiple aliases or even no aliases.</td>
</tr>
<tr>
<td>group-url [tunnel_group]</td>
<td>Displays the URLs for tunnel groups (connection profiles). You can optionally specify the name of a tunnel group to view information about that group only. Each group can have multiple URLs or even no URLs.</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays data about WebVPN events.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows output from the `show webvpn anyconnect` command:

```
> show webvpn anyconnect
1. disk0:/csm/anyconnect-win-4.2.06014-k9.pkg 1 cfg-regex=/Windows/
   CISCO STC win2k+
   4,2,06014
   Hostscan Version 4.2.06014
   Thu 10/06/2016 14:40:31.34

1 AnyConnect Client(s) installed
```

The following example shows output from the `show webvpn debug-condition` command:

```
> show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: IP address filters:
INFO: 10.100.10.10/32
```

The following example shows output from the `show webvpn group-alias` command:

```
> show webvpn group-alias
```
The following example shows output from the `show webvpn group-url` command:

```
> show webvpn group-url
http://www.cisco.com
https://ger1.example.com
https://ger2.example.com
```

The following example shows output from the `show webvpn statistics` command:

```
> show webvpn statistics
Total number of objects served 0
  html 0
  js 0
  css 0
  vb 0
  java archive 0
  java class 0
  image 0
  undetermined 0
Server compression statistics
  Decompression success from server 0
  Unsolicited compression from server 0
  Unsupported compression algorithm used by server 0
  Decompression failure for server responses 0
IOBuf failure statistics
  uib_create_with_channel 0
  uib_create_with_string 0
  uib_create_with_string_and_channel 0
  uib_transfer 0
  uib_add_filter 0
  uib_yyread 0
  uib_read 0
  uib_set_buffer_max 0
  uib_set_eof_symbol 0
  uib_get_capture_handle 0
  uib_set_capture_handle 0
  uib_buflen 0
  uib_bufptr 0
  uib_buf_endptr 0
  uib_get_buf_offset 0
  uib_get_buf_offset_addr 0
  uib_get_nth_char 0
  uib_consume 0
  uib_advance_bufptr 0
  uib_eof 0
```
show xlate

To display information about NAT sessions (xlates or translations), use the show xlate command.

show xlate [global ip1 [-ip2] [netmask mask]] [local ip1 [-ip2] [netmask mask]] [gport port1 [-port2]] [lport port1 [-port2]] [interface if_name] [type type]

Syntax Description:
- **count**: Displays the translation count.
- **global ip1[-ip2]**: (Optional) Displays the active translations by mapped IP address or range of addresses.
- **gport port1[-port2]**: Displays the active translations by the mapped port or range of ports.
- **interface if_name**: (Optional) Displays the active translations by interface.
- **local ip1[-ip2]**: (Optional) Displays the active translations by real IP address or range of addresses.
- **lport port1[-port2]**: Displays the active translations by real port or range of ports.
- **netmask mask**: (Optional) Specifies the network mask to qualify the mapped or real IP addresses.
- **type type**: (Optional) Displays the active translations by type. You can enter one or more of the following types:
  - static
  - portmap
  - dynamic
  - twice-nat (otherwise known as manual NAT)
  When specifying more than one type, separate the types with a space.

Command History:
- **Release 6.1**: This command was introduced.

Usage Guidelines:
The show xlate command displays the contents of the translation slots. The xlates can include those generated for internal interfaces, which do not appear in the NAT rules table in the device manager. These are required for internal processing.

When the VPN client configuration is enabled and the inside host is sending out DNS requests, the show xlate command may list multiple xlates for a static translation.

In a clustering environment, up to three xlates might be duplicated to different nodes in the cluster to handle a PAT session. One xlate is created on the unit that owns the connection. One xlate is created on a different unit to back up the PAT address. Finally, one xlate exists on the director that replicates the flow. In the case where the backup and director is the same unit, two instead of three xlates might be created.
Examples
The following is sample output from the `show xlate` command. The initial PAT xlates for nlp_int_tap relate to HTTPS access rules that allow Firepower Device Manager access to 192.168.1.1 rather than the management interface address. These are internal NAT xlates whose rules do not show up in the NAT table in the device manager.

```
> show xlate
13 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_2:192.168.1.1 443-443
  flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_3:192.168.1.1 443-443
  flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_4:192.168.1.1 443-443
  flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_5:192.168.1.1 443-443
  flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_6:192.168.1.1 443-443
  flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_7:192.168.1.1 443-443
  flags sr idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_8:0.0.0.0/0
  flags sIT idle 0:30:10 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_7:0.0.0.0/0
  flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_6:0.0.0.0/0
  flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_5:0.0.0.0/0
  flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_4:0.0.0.0/0
  flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_3:0.0.0.0/0
  flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_2:0.0.0.0/0
  flags sIT idle 124:39:20 timeout 0:00:00
```

The following is sample output from the `show xlate` command showing a translation from IPv4 to IPv6.

```
> show xlate
14 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
(...other entries removed...)
NAT from outside:0.0.0.0/0 to inside1_8:2001:db8::/96
  flags s idle 0:01:36 timeout 0:00:00
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear xlate</td>
<td>Clears current translation and connection information.</td>
</tr>
<tr>
<td>show conn</td>
<td>Displays all active connections.</td>
</tr>
<tr>
<td>show local-host</td>
<td>Displays the local host network information.</td>
</tr>
</tbody>
</table>
show zone

To display traffic zone information, use the `show zone` command.

```
show zone  [name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>(Optional) The name of a traffic zone.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Traffic zones are not exactly the same as security zones. Although passive security zones are also automatically generated as traffic zones, routed and switched security zones are not. Traffic zones are used for traffic load balancing (using Equal Cost Multi-Path (ECMP) routing), route redundancy, and asymmetric routing across multiple interfaces.

To view the rest of the zone configuration, use the `show running-config zone` and `show running-config interface` commands.

**Examples**

The following example displays the configured traffic zones. In this example, the traffic zone is for passive interfaces. If the zone was for Equal Cost Multi-Path routing, the zone type would be `ecmp`. The interface configuration follows. The `zone-member` command configures the interface as a member of the zone.

```
> show zone passive-security-zone
Zone: passive-security-zone passive
  Security-level: 0
  Zone member(s): 1
    passive GigabitEthernet0/0

> show running-config interface gigabitethernet0/0
! interface GigabitEthernet0/0
  mode passive
  nameif passive
  cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
  zone-member krjones-passive-security-zone
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear conn zone</td>
<td>Clears zone connections.</td>
</tr>
<tr>
<td>clear local-host zone</td>
<td>Clears zone hosts.</td>
</tr>
<tr>
<td>show interface</td>
<td>Displays the runtime status and statistics of interfaces.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>show local-host zone</td>
<td>Shows the network states of local hosts within a zone.</td>
</tr>
<tr>
<td>show nameif zone</td>
<td>Shows the zone or inline set membership for interfaces.</td>
</tr>
</tbody>
</table>
**shun**

To block connections from an attacking host, use the **shun** command. To disable a shun, use the **no** form of this command.

```
shun source_ip [dest_ip source_port dest_port [protocol] [vlan vlan_id]]
no shun source_ip [vlan vlan_id]
```

**Syntax Description**

- **dest_port** *(Optional)* Specifies the destination port of a current connection that you want to drop when you place the shun on the source IP address.

- **dest_ip** *(Optional)* Specifies the destination address of a current connection that you want to drop when you place the shun on the source IP address.

- **protocol** *(Optional)* Specifies the IP protocol of a current connection that you want to drop when you place the shun on the source IP address, such as UDP or TCP. By default, the protocol is 0 (any protocol).

- **source_ip** Specifies the address of the attacking host. If you only specify the source IP address, all future connections from this address are dropped; current connections remain in place. To drop a current connection and also place the shun, specify the additional parameters of the connection. Note that the shun remains in place for all future connections from the source IP address, regardless of destination parameters.

- **source_port** *(Optional)* Specifies the source port of a current connection that you want to drop when you place the shun on the source IP address.

- **vlan vlan_id** *(Optional)* Specifies the VLAN ID where the source host resides.

**Command Default**

The default protocol is 0 (any protocol).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **shun** command lets you block connections from an attacking host. All future connections from the source IP address are dropped and logged until the blocking function is removed manually. The blocking function of the **shun** command is applied whether or not a connection with the specified host address is currently active.

If you specify the destination address, source and destination ports, and the protocol, then you drop the matching connection as well as placing a shun on all future connections from the source IP address; all future connections are shunned, not just those that match these specific connection parameters.

You can only have one **shun** command per source IP address.

Because the **shun** command is used to block attacks dynamically, it is not displayed in the Firepower Threat Defense device configuration.

Whenever an interface configuration is removed, all shuns that are attached to that interface are also removed.
Examples
The following example shows that the offending host (10.1.1.27) makes a connection with the victim (10.2.2.89) with TCP. The connection in the Firepower Threat Defense device connection table reads as follows:

10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP

Apply the **shun** command using the following options:

```bash
> shun 10.1.1.27 10.2.2.89 555 666 tcp
Shun 10.1.1.27 added in context: single_vf
Shun 10.1.1.27 successful
```

The command deletes the specific current connection from the Firepower Threat Defense device connection table and also prevents all future packets from 10.1.1.27 from going through the Firepower Threat Defense device.

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear shun</td>
<td>Disables all the shuns that are currently enabled and clears the shun statistics.</td>
</tr>
<tr>
<td>show conn</td>
<td>Shows all active connections.</td>
</tr>
<tr>
<td>show shun</td>
<td>Displays the shun information.</td>
</tr>
</tbody>
</table>
shutdown

To shut down the device, use the **shutdown** command.

```
shutdown
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example is sample output from the **shutdown** command when you shut down the device:

```
> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': YES
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reboot</td>
<td>Reboots the device.</td>
</tr>
</tbody>
</table>
system access-control clear-rule-counts

To reset the access control rule hit count to 0, use the `system access-control clear-rule-counts` command.

```plaintext
system access-control clear-rule-counts

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example shows output from the `system access-control clear-rule-counts` command:

```plaintext
> system access-control clear-rule-counts
Are you sure that you want to clear the rule hit counters? (y/n): y
Clearing the rule hit counters.
Success.
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-control-config</td>
<td>Shows the access control policy summary and hit counts.</td>
</tr>
</tbody>
</table>
system generate-troubleshoot

To generate troubleshooting data for analysis by Cisco Technical Support when requested to do so, use the system generate troubleshoot command.

system generate-troubleshoot  options

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>options</th>
</tr>
</thead>
<tbody>
<tr>
<td>The type of troubleshooting data you want to generate display. You can enter one or more option. Use spaces to separate multiple options.</td>
<td></td>
</tr>
<tr>
<td>* ALL—Run all of the following options.</td>
<td></td>
</tr>
<tr>
<td>* SNT—Snort performance and configuration.</td>
<td></td>
</tr>
<tr>
<td>* PER—Hardware performance and logs.</td>
<td></td>
</tr>
<tr>
<td>* SYS—System configuration, policy, and logs.</td>
<td></td>
</tr>
<tr>
<td>* DES—Detection configuration, policy, and logs.</td>
<td></td>
</tr>
<tr>
<td>* NET—Interface and network related data.</td>
<td></td>
</tr>
<tr>
<td>* VDB—Discovery, awareness, VDB data, and logs.</td>
<td></td>
</tr>
<tr>
<td>* UPG—Upgrade data and logs.</td>
<td></td>
</tr>
<tr>
<td>* DBO—All database data.</td>
<td></td>
</tr>
<tr>
<td>* LOG—All log data.</td>
<td></td>
</tr>
<tr>
<td>* NMP—Network map information.</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to generate troubleshooting data for Snort and hardware performance.

> system generate-troubleshoot SNT PER
Starting /usr/local/sf/bin/sf_troubleshoot.pl...
P lease, be patient. This may take several minutes.
the troubleshoot options codes specified are SNT,PER.
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/index]
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/base-6.2.0]
Troubleshooting information successfully created at /ngfw/var/common/results-10-14-2016--181112.tar.gz
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy</td>
<td>Copies files from or to the system.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes files from the system.</td>
</tr>
</tbody>
</table>
system lockdown-sensor

To remove access to expert mode and the Bash shell, use the `system lockdown-sensor` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

**Caution**

You cannot reverse this command. If you need to restore access to expert mode, you must contact the Cisco Technical Assistance Center and get a hotfix.

The `expert` command provides access to the Bash shell, which provides administrative users extensive access to the system's operating environment. Security certification regimes (such as Common Criteria (CC) or the Unified Capabilities Approved Products List (UC APL)) impose requirements that limit the access and information available to users of a system. Use the `system lockdown-sensor` command to remove access to the `expert` command to help meet these certification requirements.

**Note**

After using this command, the `expert` command remains available in the current SSH session. You must log out and log back in to verify that the command has been removed and no longer works. Anyone else who logs in after you use the command will not be able to use expert mode either.

### Example

The following example removes access to expert mode to comply with security requirements.

```
> system lockdown-sensor
This action will remove the 'expert' command from your system for all future CLI sessions, rendering the bash shell inaccessible.

This cannot be reversed without a support call.
Continue and remove the 'expert' command?
Please enter 'YES' or 'NO': YES
>
```
system support commands

Most system support commands are used for debugging and troubleshooting at the assistance of the Cisco Technical Assistance Center. You should use the commands under the direction of Cisco support, with the exception of the following commands, which are of general use.

- system support diagnostic-cli, on page 942
- system support view-files, on page 947
- system support ssl-hw- commands, on page 944
system support ssl-client-hello- commands

These commands allow you to determine the behavior of Transport Layer Security (TLS) 1.3 downgrade to TLS 1.2. Because managed devices do not support TLS 1.3 encryption or decryption, TLS 1.3 sessions between a client and server can break, resulting in errors like the following in the client web browser:

- **ERR_SSL_PROTOCOL_ERROR**
- **SEC_ERROR_BAD_SIGNATURE**
- **ERR_SSL_VERSION_INTERFERENCE**

Errors can occur when a client connects to a server and TLS inspection determines that the connection, which has been modified to downgrade, matches a Do Not Decrypt SSL rule action.

We recommend you use these commands after consulting with Cisco TAC.

```
system support ssl-client-hello-enabled aggressive-tls13-downgrade { true | false }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>true</strong></td>
<td>Default. TLS 1.3 connections are downgraded whenever necessary to perform decryption. However, if data received after the ClientHello message causes the session to match a Do Not Decrypt rule, the session might fail.</td>
</tr>
<tr>
<td><strong>false</strong></td>
<td>TLS 1.3 connections are downgraded only when there is a reasonable certainty the session will not match a Do Not Decrypt rule. In some cases, TLS connections that need to be decrypted might not be downgraded. In those cases, traffic is not decrypted. The action specified in the SSL policy for Session not cached setting for its Undecryptable Action is taken instead.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.3.7</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
system support diagnostic-cli

To enter the diagnostic CLI, which includes additional show and other troubleshooting commands, use the `system support diagnostic-cli` command.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The Diagnostic CLI contains additional show and other commands you can use to troubleshoot the system. The commands in the Diagnostic CLI are from ASA Software. The regular Firepower Threat Defense CLI contains many of the same commands, so you might not need the extra commands of the Diagnostic CLI.

When you enter the Diagnostic CLI, you are in a separate session from the regular Firepower Threat Defense CLI.

The prompt changes to include the system hostname. There are two modes, and the prompt indicates the mode you are in. For User EXEC mode, the prompt is:

```
hostname>
```

For Privileged EXEC mode, also known as Enable mode, the prompt is the following. You enter this mode using the `enable` command. Although you are prompted for a password, simply press Enter, by default there is no password required to enter this mode.

```
hostname#
```

Keep the following tips in mind when using the Diagnostic CLI:

- To exit the Diagnostic CLI and return to the regular CLI, press `Ctrl+a`, then `d`.

- Use the `exit` command to leave Privileged EXEC mode.

The commands available in each mode differ. Privileged EXEC mode includes significantly more commands than User EXEC mode. Use `?` to see the available commands. You can find usage information in the ASA Software command references:


• The Diagnostic CLI can include commands that are not meaningful for Firepower Threat Defense. If you try a command that does not provide meaningful (or any) information, the related feature might not be configured or supported by Firepower Threat Defense.

• The Diagnostic CLI does not allow you to enter configuration mode. You cannot use the CLI to configure the device.

• When you detach from the Diagnostic CLI, the next time you enter it you are placed in the same mode you were in when you last detached.

• On the ASA 5506W-X, you can use the `session wlan` command to open a connection to the wireless module, and use its CLI to configure the access point. You must be in Privileged EXEC mode.

**Examples**

The following example shows how to enter the Diagnostic CLI and Privileged EXEC mode. When you get the password prompt after entering the `enable` command, simply press Enter. By default, there is no password to enter Privileged EXEC mode.

```bash
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```
**system support ssl-hw- commands**

These commands allow you to perform various operations on a feature referred to as *TLS/SSL hardware acceleration* in versions 6.2.3 and 6.3 and as *TLS crypto acceleration* in version 6.4. The available keywords depend on the FTD software version.

Supported devices and whether or not the feature is enabled or disabled by default also depend on software version. For this information, refer to the *Firepower Management Center Configuration Guide*.

Syntax for versions 6.2.3 and 6.3:

```
system support { ssl-hw-status | ssl-hw-supported-ciphers | ssl-hw-offload enable | ssl-hw-offload disable }
```

Syntax for version 6.4:

```
system support ssl-hw-supported-ciphers
```

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th><strong>ssl-hw-status</strong></th>
<th>Displays the current status of SSL hardware acceleration. The default state is:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• 6.2.3: disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 6.3 and 6.4: enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ssl-hw-supported-ciphers</strong></th>
<th>Displays the list of ciphers supported by SSL hardware acceleration. This command is useful because SSL hardware acceleration doesn't support all of the ciphers supported by SSL software acceleration (in particular, decryption of SEED and Camellia ciphers is not supported).</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>ssl-hw-offload enable</strong></th>
<th>Enables SSL hardware acceleration; you are prompted to reboot the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ssl-hw-offload disable</strong></td>
<td>Disables SSL hardware acceleration; you are prompted to reboot the device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Command History</strong></th>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.4</td>
<td>The feature name changed from TLS/SSL hardware acceleration to TLS crypto acceleration. The following keywords have been removed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ssl-hw-offload enable</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ssl-hw-offload disable</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ssl-hw-status</strong></td>
</tr>
<tr>
<td></td>
<td>6.3</td>
<td>The feature is enabled by default.</td>
</tr>
<tr>
<td></td>
<td>6.2.3</td>
<td>This command was introduced. The feature is disabled by default.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Note

Of the commands discussed in this section, only `system support ssl-hw-offload-supported ciphers` applies to version 6.4.

Use these commands to display information about SSL hardware acceleration or to enable or disable the feature.

Enable SSL hardware acceleration to improve encryption and decryption performance.

Disable SSL hardware acceleration to use any of the features it does not support or if you encounter unexpected traffic interruptions with an enabled SSL policy.

Features not supported by SSL hardware acceleration include the following:

- If the inspection engine is configured to preserve connections and the inspection engine fails unexpectedly, TLS/SSL traffic is dropped until the engine restarts.

  This behavior is controlled by the `configure snort preserve-connection {enable | disable}` command.

Use the `system support ssl-hw-status` command to display the current status.

Use the `system support ssl-hw-supported-ciphers` command to display the list of ciphers supported by SSL hardware acceleration.

Examples

Following is an example of viewing the current status of SSL hardware acceleration:

```
> system support ssl-hw-status
Hardware Offload configuration set to Disabled
```

Following is an example of enabling SSL hardware acceleration with prompting to reboot the device:

If you enable SSL hardware acceleration, you cannot:

1. Decrypt passive or inline tap traffic.
2. Preserve Do Not Decrypt connections when the inspection engine restarts.

Continue? (y/n) [n]: y

Enabling or disabling SSL hardware acceleration reboots the system. Continue? (y/n) [n]: y

SSL hardware acceleration will be enabled on system boot.

You are required to confirm all of the preceding before the device is rebooted.

Following is a partial list of the ciphers supported by SSL hardware acceleration:

```
> system support ssl-hw-supported-ciphers

CID   Cipher Suite Name   CH_mod Keep  Support Inline
Support Passive
--------------------------------------------------------------------------------------------------------
0x0004 TLS_RSA_WITH_RC4_128_MD5       Yes    Yes    Yes
0x0005 TLS_RSA_WITH_RC4_128_SHA      Yes    Yes    Yes
0x0009 TLS_RSA_WITH_DES_CBC_SHA      Yes    Yes    Yes
```
<table>
<thead>
<tr>
<th>Code</th>
<th>Algorithm</th>
<th>SSL</th>
<th>TLS</th>
<th>SSH</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00a</td>
<td>TLS_RSA_WITH_3DES_EDE_CBC_SHA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>0x00c</td>
<td>TLS_DH_DSS_WITH_DES_CBC_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x00d</td>
<td>TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x00f</td>
<td>TLS_DH_RSA_WITH_DES_CBC_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x010</td>
<td>TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x012</td>
<td>TLS_DHE_DSS_WITH_DES_CBC_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x013</td>
<td>TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x015</td>
<td>TLS_DHE_RSA_WITH_DES_CBC_SHA</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>0x016</td>
<td>TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>0x018</td>
<td>TLS_DH_Anon_WITH_RC4_128_MD5</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>0x01a</td>
<td>TLS_DH_Anon_WITH_DES_CBC_SHA</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>0x01b</td>
<td>TLS_DH_Anon_WITH_3DES_EDE_CBC_SHA</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>0x01e</td>
<td>TLS_KRB5_WITH_DES_CBC_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x01f</td>
<td>TLS_KRB5_WITH_3DES_EDE_CBC_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x020</td>
<td>TLS_KRB5_WITH_RC4_128_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x024</td>
<td>TLS_KRB5_WITH_RC4_128_MD5</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x02f</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>0x030</td>
<td>TLS_DH_DSS_WITH_AES_128_CBC_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0x031</td>
<td>TLS_DH_RSA_WITH_AES_128_CBC_SHA</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

...more
system support view-files

To view system log contents when working with the Cisco Technical Assistance Center (TAC) to resolve a problem, use the system support view-files command.

**system support view-files**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The system support view-files command opens a system log. Use this command while working with the Cisco Technical Assistance Center (TAC) so that they can help you interpret the output and to select the appropriate log to view.

The command presents a menu for selecting a log. Use the following commands to navigate the wizard:

- To change to a sub-directory, type in the name of the directory and press Enter.
- To select a file to view, enter s at the prompt. You are then prompted for a file name. You must type the complete name, and capitalization matters. The file list shows you the size of the log, which you might consider before opening very large logs.
- Press the space bar when you see --More-- to see the next page of log entries; press Enter to see just the next log entry. When you reach the end of the log, you are taken to the main menu. The --More-- line shows you the size of the log and how much of it you have viewed. Use Ctrl+C to close the log and exit the command if you do not want to page through the entire log.
- Type b to go up one level in the structure to the menu.

If you want to leave the log open so you can see new messages as they are added, use the tail-logs command.

**Examples**

The following example shows how view the ngfw.log file. The file listing starts with directories at the top, then a list of files in the current directory.

```
> system support view-files
---View Logs---

Directory: /ngfw/var/log
---------sub-dirs---------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tail-logs</td>
<td>Opens a log and keeps it open.</td>
</tr>
</tbody>
</table>
PART III

T - Z Commands

• t - z, on page 951
t - z

- tail-logs, on page 952
- test aaa-server, on page 954
- traceroute, on page 956
- undebug, on page 959
- verify, on page 960
- vpn-sessiondb logoff, on page 964
- write net, on page 965
- write terminal, on page 966
**tail-logs**

To open a system log to view messages as they are written when working with the Cisco Technical Assistance Center (TAC) to resolve a problem, use the `tail-logs` command.

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `tail-logs` command opens a system log so that you can see messages as they are written. Use this command while working with the Cisco Technical Assistance Center (TAC) so that they can help you interpret the output and to select the appropriate log to view.

The command presents a menu listing all available logs. Follow the command prompts to select the log. If the log is long, you will see a `More` line; press `Enter` to progress a line at a time, `Space` to go a page at a time. Press `Ctrl+C` to return to the command prompt when you are finished viewing the log.

**Examples**

The following example shows how tail the `ngfw.log` file. The file listing starts with directories at the top, then a list of files in the current directory.

```
> tail-logs
===Tail Logs===
-------------------------------
Directory: /ngfw/var/log
---------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
af
scripts
packages
removed_scripts
httpd
---------files----------
2016-10-14 18:12:04.514783 | 5371 | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353 | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517 | action_queue.log
2016-10-06 16:00:56.620019 | 1018 | br1.down.log
<list abbreviated>
2016-10-06 15:38:22.630001 | 9194 | ngfw.log
<list abbreviated>

[b] to go back or [s] to select a file to view, [Ctrl+C] to exit
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> ngfw.log
2016-10-06 15:38:22 Running [rm -rf /etc/logrotate-dmesg.conf /etc/logrotate.conf
/etc/logrotate.d
/etc/logrotate_ssp.conf /etc/logrotate_ssp.d] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate-size.conf /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate-size.d /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate.conf /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate.d /etc/] ... success
2016-10-06 15:38:22 Running [rm -f /usr/sbin/ntpd] ... success

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>system support view-files</td>
<td>Opens a log file.</td>
</tr>
</tbody>
</table>
test aaa-server

To check whether the device can authenticate or authorize users with a particular AAA server, use the `test aaa-server` command.

```
test aaa-server {authentication groupname [host ip_address] [username username] [password password] | authorization groupname [host ip_address] [username username]}
```

**Syntax Description**
- `groupname`: Specifies the AAA server group or realm name.
- `host ip-address`: Specifies the server IP address. If you do not specify the IP address in the command, you are prompted for it.
- `password password`: Specifies the user password. If you do not specify the password in the command, you are prompted for it.
- `username username`: Specifies the username of the account used to test the AAA server settings. Make sure the username exists on the AAA server; otherwise, the test will fail. If you do not specify the username in the command, you are prompted for it.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command lets you verify that the system can authenticate or authorize users with a particular AAA server. This command lets you test the AAA server without having an actual user attempt to authenticate. It also helps you isolate whether AAA failures are due to misconfiguration of AAA server parameters, a connection problem to the AAA server, or other configuration errors.

**Examples**

The following is an example of a successful authentication:

```
> test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

The following is an unsuccessful authentication attempt:

```
> test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Rejected: Unspecified
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa-server active</td>
<td>Reactivate a AAA server that is marked failed or fail an active AAA server.</td>
</tr>
<tr>
<td></td>
<td>aaa-server fail</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear aaa-server statistics</td>
<td>Clears AAA server statistics.</td>
</tr>
<tr>
<td></td>
<td>show aaa-server</td>
<td>Displays AAA server statistics.</td>
</tr>
</tbody>
</table>
# traceroute

To determine the route packets will take to their destination through data interfaces, use the `traceroute` command. To determine the route packets will take to their destination when going through the management IP address, use the `traceroute system` command.

```
traceroute destination [source {source_ip | source-interface}] [numeric] [timeout timeout_value] [probe probe_num] [ttl min_ttl max_ttl] [port port_value] [use-icmp]
traceroute system destination
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>destination</strong></td>
<td>The IPv4 or IPv6 address, or hostname, of the host to which the route is to be traced. For example, 10.100.10.10 or <a href="http://www.example.com">www.example.com</a>. You must configure a DNS server to resolve a hostname. Traces that use the <code>system</code> keyword use the DNS servers configured for the management interface. Other traces use the DNS servers configured for the data interfaces. If you do not have DNS defined for the data interfaces, first use the <code>nslookup</code> command to determine the host’s IP address, and then use the IP address instead of the FQDN.</td>
</tr>
<tr>
<td><strong>numeric</strong></td>
<td>Specifies the output print only the IP addresses of the intermediate gateways. If this keyword is not specified the traceroute attempts to look up the hostnames of the gateways reached during the trace.</td>
</tr>
<tr>
<td><strong>port port_value</strong></td>
<td>The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434.</td>
</tr>
<tr>
<td><strong>probe probe_num</strong></td>
<td>The number of probes to be sent at each TTL level. The default count is 3.</td>
</tr>
<tr>
<td>**source {source_ip</td>
<td>source_interface}**</td>
</tr>
<tr>
<td><strong>system</strong></td>
<td>Indicates the traceroute should be through the management interface, not a data interface.</td>
</tr>
<tr>
<td><strong>timeout timeout_value</strong></td>
<td>Specifies the amount of time in seconds to wait for a response before the connection times out. The default is three seconds.</td>
</tr>
<tr>
<td><strong>ttl min_ttl max_ttl</strong></td>
<td>Specifies the range of Time To Live values to use in the probes.</td>
</tr>
<tr>
<td></td>
<td>• <code>min_ttl</code>—The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.</td>
</tr>
<tr>
<td></td>
<td>• <code>max-ttl</code>—The largest TTL value that can be used. The default is 30. The command terminates when the traceroute packet reaches the destination or when the value is reached.</td>
</tr>
<tr>
<td><strong>use-icmp</strong></td>
<td>Specifies the use of ICMP probe packets instead of UDP probe packets.</td>
</tr>
</tbody>
</table>

Cisco Firepower Threat Defense Command Reference
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **traceroute** command prints the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. The following are the output symbols printed by the **traceroute** command:

<table>
<thead>
<tr>
<th>Output Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>No response was received for the probe within the timeout period.</td>
</tr>
<tr>
<td>nn msec</td>
<td>For each node, the round-trip time (in milliseconds) for the specified number of probes.</td>
</tr>
<tr>
<td>!N.</td>
<td>ICMP network unreachable.</td>
</tr>
<tr>
<td>!H</td>
<td>ICMP host unreachable.</td>
</tr>
<tr>
<td>!P</td>
<td>ICMP protocol unreachable.</td>
</tr>
<tr>
<td>!A</td>
<td>ICMP administratively prohibited.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown ICMP error.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows traceroute output that results when a destination IP address has been specified:

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
1  10.83.194.1 0 msec 10 msec 0 msec
2  10.83.193.65 0 msec 0 msec 0 msec
3  10.88.193.101 0 msec 10 msec 0 msec
4  10.88.193.97 0 msec 0 msec 10 msec
5  10.88.239.9 0 msec 10 msec 0 msec
6  10.88.238.65 10 msec 10 msec 0 msec
7  172.16.7.221 70 msec 70 msec 80 msec
8  209.165.200.225 70 msec 70 msec 70 msec
```

The following example shows a traceroute through the management interface to a hostname.

```
> traceroute system www.example.com
trace route to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10 corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11 dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture</td>
<td>Captures packet information, including trace packets.</td>
</tr>
<tr>
<td>show capture</td>
<td>Displays the capture configuration when no options are specified.</td>
</tr>
<tr>
<td>packet-tracer</td>
<td>Enables packet tracing capabilities.</td>
</tr>
</tbody>
</table>
To disable debugging for a given feature, use the `undebug` command. This command is a synonym for the `no debug` command.

```
undebug {feature [subfeature] [level] | all}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Disables debugging for all features.</td>
</tr>
<tr>
<td><code>feature</code></td>
<td>Specifies the feature for which you want to disable debugging. To see available features, use the <code>undebug ?</code> command for CLI help.</td>
</tr>
<tr>
<td><code>subfeature</code></td>
<td>(Optional) Depending on the feature, you can disable debug messages for one or more subfeatures. Use ? to see the available subfeatures.</td>
</tr>
<tr>
<td><code>level</code></td>
<td>(Optional) Specifies the debugging level. The level might not be available for all features. Use ? to see the available levels.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use `debug` commands only to troubleshoot specific problems or during troubleshooting sessions with the Cisco Technical Assistance Center (TAC). Moreover, it is best to use `debug` commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased `debug` command processing overhead will affect system use.

You can view debug output in a CLI session only. Output is directly available when connected to the Console port, or when in the diagnostic CLI (enter `system support diagnostic-cli`). You can also view output from the regular Firepower Threat Defense CLI using the `show console-output` command.

### Example

The following example disables debugging for all enabled debugs.

```
> undebug all
>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug</td>
<td>Enables debugging for a feature.</td>
</tr>
<tr>
<td>show debug</td>
<td>Shows the currently active debug settings.</td>
</tr>
</tbody>
</table>
verify

To verify the checksum of a file, use the `verify` command.

```
verify [sha-512 | /signature] path
verify/md5 path [md5-value]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/md5</code></td>
<td>(Optional) Calculates and displays the MD5 value for the specified software image. Compare this value with the value available on Cisco.com for this image.</td>
</tr>
<tr>
<td><code>sha-512</code></td>
<td>(Optional) Calculates and displays the SHA-512 value for the specified software image. Compare this value with the value available on Cisco.com for this image.</td>
</tr>
<tr>
<td><code>/signature</code></td>
<td>(Optional) Verifies the signature of an image stored in flash.</td>
</tr>
<tr>
<td><code>md5-value</code></td>
<td>(Optional) The known MD5 value for the specified image. When an MD5 value is specified in the command, the system will calculate the MD5 value for the specified image and display a message verifying that the MD5 values match or that there is a mismatch.</td>
</tr>
</tbody>
</table>
filename

The name of a file in the current directory. Use dir to see directory contents, cd to change directories.

- **disk0:**[/path]/filename

  This option indicates the internal Flash memory. You can also use flash: instead of disk0; they are aliased.

- **disk1:**[/path]/filename

  This option indicates the external Flash memory card.

- **flash:**[/path]/filename

  This option indicates the internal Flash card. For the ASA 5500 series, flash is an alias for disk0:

- **ftp://[user[:password]@[server[: port]]/][path]/filename:[type=xx]

  The type can be one of the following keywords:
  - **ap**—ASCII passive mode
  - **an**—ASCII normal mode
  - **ip**—(Default) Binary passive mode
  - **in**—Binary normal mode

- **http[s]://[user[:password]@[server[: port]]/][path]/filename

- **tftp://[user[:password]@[server[: port]]/][path]/filename[:int=interface_name]

  Specify the interface name if you want to override the route to the server address. The pathname cannot contain spaces.

---

**Command Default**

The current flash device is the default file system.

---

**Note**

When you specify the /md5 option, you can use a network file, such as ftp, http and tftp as the source. The verify command without the /md5 option only lets you verify local images in Flash.

---

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the verify command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into Flash memory; it is not displayed when the image file is copied from one disk to another.
Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into Flash memory or onto a server. A variety of image information is available on Cisco.com.

To display the contents of Flash memory, use the `show flash:` command. The Flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into Flash memory, use the `verify` command. Note, however, that the `verify` command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the device and saved in the file system without detection. If a corrupt image is transferred successfully to the device, the software will be unable to tell that the image is corrupted and the file will verify successfully.

To use the message-digest5 (MD5) hash algorithm to ensure file validation, use the `verify` command with the `/md5` option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The `/md5` option of the `verify` command allows you to check the integrity of the security appliance software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all security appliance software images for comparison against local system image values.

To perform the MD5 integrity check, issue the `verify` command using the `/md5` keyword. For example, issuing the `verify /md5 flash:cdisk.bin` command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, issuing the `verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae7257140f962233` command will display a message verifying that the MD5 values match or that there is a mismatch. A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

**Examples**

The following example verifies an image file. This is the same result you would see if you included the `/signature` keyword.

```
> verify os.img
Verifying file integrity of disk0:/os.img
Computed Hash    SHA2: 4916c9b70ad368f6e02a0597f6ef798e
                 ca360037fc0bb596c78e7ef916c6c398
e238e2597eab2135c48161df3e6f4a7
                 66e4ec15a7b327ee26963b2fd6e2b347
Embedded Hash   SHA2: 4916c9b70ad368f6e02a0597f6ef798e
c360037fc0bb596c78e7ef916c6c398
e238e2597eab2135c48161df3e6f4a7
                 66e4ec15a7b327ee26963b2fd6e2b347
Digital signature successfully validated
```

The following example calculates an MD5 value for the image. Most exclamation points have been removed for brevity.

```
> verify /md5 os.img
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
verify /MD5 (disk0:/os.img) = 0940c6c71d3d43b3ba495f7290f4f276
```
The following example calculates an MD5 value and compares it to the expected value. The decision in this case is Verified, the calculated and expected values match.

```
> verify /md5 os.img 0940c6c71d3d43b3ba495f7290f4f276
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Done!
Verified (disk0:/os.img) = 0940c6c71d3d43b3ba495f7290f4f276
```

The following example computes the SHA-512 value for the image.

```
> verify /sha-512 os.img
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Done!
verify /SHA-512 (disk0:/os.img) = 77421c0f6498976feb530e62bd8b9e8140b52a851f055265080a392299848a77227d6047827192f3d4969d36944abf2bddd215ec4127f9503173f82a2d6c7e2
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy</td>
<td>Copies files.</td>
</tr>
<tr>
<td>dir</td>
<td>Lists the files in the system.</td>
</tr>
</tbody>
</table>
vpn-sessiondb logoff

To log off all or selected VPN sessions, use the `vpn-sessiondb logoff` command.

```
vpn-sessiondb logoff { all | index index_number | ipaddress IPaddr | l2l | name username | protocol protocol-name | tunnel-group groupname } noconfirm
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Logs off all VPN sessions.</td>
</tr>
<tr>
<td><code>index index_number</code></td>
<td>Logs off a single session by index number. You can view index numbers for each session with the <code>show vpn-sessiondb detail</code> command.</td>
</tr>
<tr>
<td><code>ipaddress IPaddr</code></td>
<td>Logs off sessions for the IP address that you specify.</td>
</tr>
<tr>
<td><code>l2l</code></td>
<td>Logs off all LAN-to-LAN sessions.</td>
</tr>
<tr>
<td><code>name username</code></td>
<td>Logs off sessions for the username that you specify.</td>
</tr>
<tr>
<td><code>protocol protocol-name</code></td>
<td>Logs off sessions for protocols that you specify. The protocols include:</td>
</tr>
<tr>
<td></td>
<td>• <code>ikev1</code>—Internet Key Exchange version 1 (IKEv1) sessions.</td>
</tr>
<tr>
<td></td>
<td>• <code>ikev2</code>—Internet Key Exchange version 2 (IKEv2) sessions.</td>
</tr>
<tr>
<td></td>
<td>• <code>ipsec</code>—IPsec sessions using either IKEv1 or IKEv2.</td>
</tr>
<tr>
<td></td>
<td>• <code>ipseclan2lan</code>—IPsec LAN-to-LAN sessions.</td>
</tr>
<tr>
<td></td>
<td>• <code>ipseclan2lanovernatt</code>—IPsec LAN-to-LAN over NAT-T sessions.</td>
</tr>
<tr>
<td><code>tunnel-group groupname</code></td>
<td>Logs off sessions for the tunnel group (connection profile) that you specify.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to log off sessions for the Corporate tunnel group (connection profile).

```
> vpn-sessiondb logoff tunnel-group Corporate noconfirm
INFO: Number of sessions from TunnelGroup "Corporate" logged off : 1
```
write net

To save the running configuration to a TFTP server, use the **write net** command.

```
write net [interface if_name] server: [filename]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>:filename</code></td>
<td>Specifies the path and filename.</td>
</tr>
<tr>
<td><code>interface if_name</code></td>
<td>The name of the interface through which the TFTP server can be reached.</td>
</tr>
<tr>
<td><code>server:</code></td>
<td>Sets the TFTP server IP address or name.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The running configuration is the configuration currently running in memory.

### Examples

The following example copies the running configuration to a TFTP server through the inside interface.

```
> write net interface inside 10.1.1.1:/configs/contextbackup.cfg
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Shows the running configuration.</td>
</tr>
</tbody>
</table>
write terminal

To show the running configuration on the terminal, use the **write terminal** command.

```
write terminal
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is equivalent to the **show running-config** command.

**Examples**

The following example writes the running configuration to the terminal:

```
> write terminal
: Saved
: Serial Number: XXXXXXXXXXX
: Hardware: ASA5516, 8192 MB RAM, CPU Atom C2000 series 2416 MHz, 1 CPU (8 cores)
: NGFW Version 6.2.0
: hostname firepower
(...remaining output deleted...)
```