show d - show h

show database

To display information about the system database, use the **show database** command.

show database {**processes** | **slow-query-log**}

Syntax Description

processes	Displays information about the currently running database queries.
slow-query-log	Displays the database slow query log.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example shows how to display database process information.

```
> 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 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

Release	Modification
6.1	This command was introduced.
6.7	For the Web update method, the output of the **interface** keyword includes the last successful updated FQDN/IP address mapping. For the **method** keyword, output for the Web update method was added.

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 shows a successful web type update:

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : ftd1.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

The following example shows a web type failure:

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available
```

```
Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

The following example shows that the DNS server returned an error for the web type update:

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

The following example shows that a web update was not yet attempted due to the IP address unconfigured or the DHCP request failed, for example:

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

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
>
```

The following example shows details about the web update method:

```
> show ddns update method web1

Dynamic DNS Update Method: web1
 Dynamic DNS updated via HTTP(s) protocols
  URL used to update record: https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
```

Related Commands

Command	Description
show running-config ddns	Displays the type and interval of all configured DDNS methods in the running configuration.

show debug

To show the current debugging configuration, use the **show debug** command.

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

Syntax Description

command	(Optional) Specifies the **debug** command whose current configuration you want to view.
keywords	(Optional) For each command, the keywords following the command are identical to the keywords supported by the associated **debug** command.

Command History

Release	Modification
6.1	This command was introduced.

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.

```
> 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

Command	Description
debug	Enables debugging.

show debug

To show the current debugging configuration, use the **show debug** command.

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

Syntax Description

command	(Optional) Specifies the **debug** command whose current configuration you want to view.
keywords	(Optional) For each command, the keywords following the command are identical to the keywords supported by the associated **debug** command.

Command History

Release	Modification
6.1	This command was introduced.

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.

```
> 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

Command	Description
debug	Enables debugging.

show dhcpd

To view DHCP binding, state, and statistical information, use the **show dhcpd** command.

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

Syntax Description

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

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

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

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 inside1_2, Configured for DHCP SERVER
Interface inside1_3, Configured for DHCP SERVER
Interface inside1_4, Configured for DHCP SERVER
Interface inside1_5, Configured for DHCP SERVER
Interface inside1_6, Configured for DHCP SERVER
Interface inside1_7, Configured for DHCP SERVER
Interface inside1_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
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

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

Related Commands

Command	Description
clear dhcpd	Clears the DHCP server bindings and statistic counters.
show running-config dhcpd	Displays the current DHCP server configuration.

show dhcprelay

To view DHCP relay agent state and statistical information, use the **show dhcprelay state** command.

show dhcprelay {**state** | **statistics**}

Syntax Description

state	Displays the state of the DHCP relay agent for each interface.
statistics	Displays DHCP relay statistics.

Command History

Release	Modification
6.1	This command was introduced.

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

Command	Description
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
show dhcpd	Displays DHCP server statistics and state information.

show diameter

To display state information for each Diameter connection, use the **show diameter** command.

show diameter

Command History

Release	Modification
6.2	This command was introduced.

Usage Guidelines

To display Diameter connection state information, you must inspect Diameter traffic. To inspect Diameter traffic, you need to configure a FlexConfig in 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

Command	Description
clear service-policy	Clears service policy statistic.

show disk

To display the contents of the flash memory for the threat defense device only, use the **show disk** command.

show disk
show {**disk0:** | **disk1:**} [**filesys** | **all** | **controller**]

Syntax Description

{**disk0:** | **disk1:**}	Specifies the internal flash memory (disk0:) or the external flash memory (disk1:). If you enter the command with no numbers, **show disk**, you see information about the file systems.
all	Shows the contents of flash memory plus the file system and controller information.
controller	Displays the flash controller model number.
filesys	Shows information about the compact flash card.

Command Default

By default, this command shows file system information.

Command History

Release	Modification
6.1	This command was introduced.

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 05 2016 02:10:26  os.img
   49  33          Oct 11 2016 21:32:16  .boot_string
   50  150484      Oct 06 2016 15:36:02  install.log
   11  4096        Oct 06 2016 15:58:16  log
   13  1544        Oct 13 2016 18:59:06  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
   56  507281      Oct 20 2016 18:10:20  crashinfo-test_20161020_181021_UTC
```

```
7935832064 bytes total (7827599360 bytes free)
```

The following is sample output from the **show disk0: filesys** command:

```
> 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:

```
> show disk0: controller

Flash Model: ATA Micron_M500DC_MT
```

Related Commands

Command	Description
dir	Displays the directory contents.

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.

show disk-manager

Command History

Release	Modification
6.1	This command was introduced.

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

host *fqdn*	Displays information about the specified fully-qualified domain name (FQDN) only.
system	Displays the DNS servers and search domain configured for the management interface.

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

Release	Modification
6.1	This command was introduced.
6.3	Support was added for FQDN-based access control rules.

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
```

```
Address: 10.1.3.3                         TTL 00:00:36
Address: 10.4.1.2                         TTL 00:01:01
```

Related Commands

Command	Description
clear dns	Removes FQDN network object DNS resolutions.
show network	Displays the configuration of the management interface.

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

Command History

Release	Modification
6.1	This command was introduced.

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 1: show dns-hosts Fields

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

Related Commands

Command	Description
clear dns-hosts	Clears the DNS cache.

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 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

Release	Modification
6.1	This command was introduced.

Usage Guidelines

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

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

The **show eigrp events type** command displays the logging status of EIGRP events. By default, neighbor changes, neighbor warning, and DUAL FSM messages are logged. You 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
```

```
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

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

```
> 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

Command	Description
clear eigrp events	Clears the EIGRP event logging buffer.

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 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

Release	Modification
6.1	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

```
> show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
mgmt          0         0/0          0      11/434          0          0
outside       1         0/0        337       0/10           0          0
inside        1         0/0         10       1/63         103          0
```

The following table describes the significant fields shown in the display.

Table 2: show eigrp interfaces Field Descriptions

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

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 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	Modification
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      4    5     20
```

The following table describes the significant fields shown in the display.

Table 3: show eigrp neighbors Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Address	IP address of the EIGRP neighbor.

Field	Description
Interface	Interface on which the threat defense device receives hello packets from the neighbor.
Holdtime	Length of time (in seconds) that the 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 threat defense device considers the neighbor unreachable.
Uptime	Elapsed time (in hours:minutes: seconds) since the threat defense device first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the threat defense device is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from the neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the threat defense device to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the threat defense device waits before resending a packet from the retransmission queue to a neighbor.

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

```
> 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 4: show ip eigrp neighbors static Field Descriptions

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

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

```
> show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0             11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0             13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0             12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

The following table describes the significant fields shown in the display.

Table 5: show ip eigrp neighbors details Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
H	This column lists the order in which a peering session was established with the specified neighbor. The order is specified with sequential numbering starting with 0.
Address	IP address of the EIGRP neighbor.
Interface	Interface on which the threat defense device receives hello packets from the neighbor.
Holdtime	Length of time (in seconds) that the 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 threat defense device considers the neighbor unreachable.
Uptime	Elapsed time (in hours:minutes: seconds) since the threat defense device first heard from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the threat defense device to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the threat defense device waits before resending a packet from the retransmission queue to a neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the threat defense device is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from the neighbor.

Field	Description
Version	The software version that the specified peer is running.
Retrans	The number of times that a packet has been retransmitted.
Retries	The number of times an attempt was made to retransmit a packet.
Restart time	Elapsed time (in hours:minutes:seconds) since the specified neighbor has restarted.

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

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

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

Release	Modification
6.1	This command was introduced.

Usage Guidelines

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

Examples

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

```
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
```

```
        via 10.16.81.28 (307200/281600), Ethernet1
        via 10.16.80.28 (307200/281600), Ethernet0
```

The following table describes the significant fields shown in the displays.

Table 6: show eigrp topology Field Information

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

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

```
> 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

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

show eigrp traffic

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

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 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 7: show eigrp traffic Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgment packets sent and received.

Field	Description
Input queue high water mark/drops	Number of received packets that are approaching the maximum receive threshold and number of dropped packets.
SIA-Queries sent/received	Stuck-in-active queries sent and received.
SIA-Replies sent/received	Stuck-in-active replies sent and received.

show elephant-flow detection-config

To show the configured parameters for elephant flow detection, use the **show elephant-flow detection-config** command.

Attention This command is supported for the management center and threat defense Version 7.1 only.

show elehpant-flow detection-config

Command History

Release	Modification
7.1	This command was introduced.

Usage Guidelines

To view the configured size and time thresholds for elephant flow detection, use the **show elephant-flow detection-config** command.

Examples

The following example shows the configured values for threshold and size for elephant flow detection.

```
> show elephant-flow detection-config
bytes_threshold(in MBs) = 50,
time_threshold(in Seconds) = 15
```

Related Commands

Command	Description
system support elephant-flow-detection	Configures the elephant flow detection parameters.
show elephant-flow status	Displays the elephant flow detection status (enabled or disabled).

show elephant-flow status

To show the elephant flow detection status (enabled or disabled), use the **show elephant-flow status** command.

Attention This command is supported for the management center and threat defense Version 7.1 only.

show elephant-flow status

Command History

Release	Modification
7.1	This command was introduced.

Usage Guidelines

To see if elephant flow detection is enabled or disabled, use the **show elephant-flow status** command.

Examples

The following example shows that elephant flow detection is enabled.

```
> show elephant-flow status
Elephant flow inspector is enabled
```

Command	Description
system support elephant-flow-detection	Configures the elephant flow detection parameters.
show elephant-flow detection-config	Displays the configured parameters for elephant flow detection.

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.

show environment [**alarm-contact** | **driver** | **fans** | **power-supplies** | **power_consumption** | **voltage** | **temperature** [**accelerator** | **chassis** | **cpu** | **io-hub** | **mother-board** | **power-supply**]]

Syntax Description

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

Release	Modification
6.1	This command was introduced.
6.3	We added the **alarm-contact** keyword for the ISA 3000.

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 Supplies:
-------------------------------------
   Power Supply Unit Redundancy: OK
   Temperature:
   --------------------------------
   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
   Left Slot (PS0): 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
```

Related Commands

Command	Description
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.
show facility-alarm	Displays status information for triggered alarms.
show version	Displays the hardware and software version.

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

relay	Displays the alarms that have energized the alarm output relay.
status [**major** | **minor** | **info**]	Displays all the alarms that have been triggered. You can add the following keywords to limit the list: • **major**—Displays all the major severity alarms. • **minor**—Displays all the minor severity alarms. • **info**—Displays all the alarms. This keyword provides the same output as using no keyword.

Command History

Release	Modification
6.3	This command was introduced.

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.

Column	Description
Source	The device from which the alarm was triggered. This is usually the hostname configured on the device.
Severity	Major or minor.
Description	The type of alarm triggered. For example, temperature, external alarm contact, or redundant power supply.
Relay	Whether the external alarm output relay was energized or de-energized. The external output alarm is triggered based on your alarm configuration.
Time	The timestamp of the triggered alarm.

Examples

The following is a sample output from the **show facility-alarm relay** command:

```
> show facility-alarm relay
Source    Severity   Description                          Relay      Time
firepower minor      external alarm contact 1 triggered  Energized  06:56:50 UTC Mon Sep
22 2014
```

The following is a sample output from the **show facility-alarm status** command:

```
> show facility-alarm status info
Source    Severity  Description                          Relay         Time
firepower minor external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep 22
2014
firepower minor Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep 22
2014
firepower major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep 22
2014
firepower major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep 22
2014

> show facility-alarm status major
Source    Severity  Description                          Relay         Time
firepower major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
22 2014
firepower major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
22 2014


> show facility-alarm status minor
Source    Severity  Description                           Relay         Time
firepower minor     external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep
 22 2014
firepower minor     Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep
 22 2014
```

Related Commands

Command	Description
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays the status of the input alarm contacts.

show failover

To display information about the failover status of a high-availability unit, use the **show failover** command.

show failover [**group** *num* | **history** [**details**] | **interface** | **state** | **trace** [*options*] | **app-sync stats** | **statistics** | **details**

Syntax Description

group *num*	Displays the running state of the specified failover group.
history [**details**]	Displays failover history. This includes past failover state changes and the reasons for the state changes. 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. Note that the history information is cleared when the device is rebooted.
interface	Displays failover and stateful link information.
state	Displays the failover state of both the failover units. The information displayed includes the primary or secondary status of the unit, the **Active** or **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.
trace [*options*]	(Optional) Shows the failover event trace. Options include the failover event trace levels from 1 to 5: • **critical** : Filters failover critical event trace (level = 1). • **debugging**: Filters failover debugging trace (debug level = 5). • **error**: Filters failover internal exception (level = 2). • **informational**: Filters failover informational trace (level = 4). • **warning**: Filters failover warnings (level = 3).
statistics	Displays transmit and receive packet count of failover command interface.
details	Displays the failover details of the pairs in a high-availability pair.

Command History

Release	Modification
6.1	This command was introduced.
6.2.3	The **history details** keyword was added.

Release	Modification
6.4	The following object static counts were added: • Rule DB B-Sync • Rule DB P-Sync • Rule DB Delete
7.0	The **details** keyword was added.

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 threat defense device up time, which the active threat defense device passes on to the standby 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 8: Failover Interface States

State	Description
Normal	The interface is up and receiving hello packets from the corresponding interface on the peer unit.
Normal (Waiting)	The interface is up but has not yet received a hello packet from the corresponding interface on the peer unit. Verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces. You can also see this state when the failover interface goes down.
Normal (Not-Monitored)	The interface is up but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
No Link	The physical link is down.
No Link (Waiting)	The physical link is down and the interface has not yet received a hello packet from the corresponding interface on the peer unit. After restoring the link, verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
No Link (Not-Monitored)	The physical link is down but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
Link Down	The physical link is up, but the interface is administratively down.

State	Description
Link Down (Waiting)	The physical link is up, but the interface is administratively down and the interface has not yet received a hello packet from the corresponding interface on the peer unit. After bringing the interface up, verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
Link Down (Not-Monitored)	The physical link is up, but the interface is administratively down but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
Testing	The interface is in testing mode due to missed hello packets from the corresponding interface on the peer unit.
Failed	Interface testing has failed and the interface is marked as failed. If the interface failure causes the failover criteria to be met, then the interface failure causes a failover to the secondary unit or failover group.

Examples

The following is a 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 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
    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)
    Stateful Obj       xmit       xerr       rcv        rerr
    General            45         0          44         0
    sys cmd            44         0          44         0
    up time            0          0          0          0
    RPC 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
              Cur   Max  Total
    Recv Q:   0     10    44
    Xmit Q:   0     11    238
```

The following is a sample output from the **show failover state** command for an active-standby setup:

```
> show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2016
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2016

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

The following table describes the output of the **show failover state** command.

Table 9: show failover state Field Descriptions

Field	Description
Configuration State	Displays the state of configuration synchronization. The following are possible configuration states for the standby unit: • **Config Syncing - STANDBY**: Set while the synchronized configuration is being executed. • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY**: Set when the standby unit has completed a configuration synchronization from the active unit. The following are possible configuration states for the active unit: • **Config Syncing**: Set on the active unit when it is performing a configuration synchronization to the standby unit. • **Interface Config Syncing** • **Sync Done**: Set when the active unit has completed a successful configuration synchronization to the standby unit. • **Ready for Config Sync**: Set on the active unit when the standby unit signals that it is ready to receive a configuration synchronization.
Communication State	Displays the status of the MAC address synchronization. • **Mac set**: The MAC addresses have been synchronized from the peer unit to this unit. • **Updated Mac**: Used when a MAC address is updated and needs to be synchronized to the other unit. Also used during the transition period where the unit is updating the local MAC addresses synchronized from the peer unit.
Date/Time	Displays a date and timestamp for the failure.
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** or **Secondary** and **Active** or **Standby** status for the unit.

Field	Description
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.

The following is a sample output from the **show failover history** command on the primary unit:

```
> show failover history
==========================================================================
From State                 To State                   Reason
==========================================================================
14:29:59 UTC Nov 11 2017
Not Detected               Negotiation                No Error

14:30:36 UTC Nov 11 2017
Negotiation                Cold Standby               Detected an Active mate

14:30:38 UTC Nov 11 2017
Cold Standby               Sync Config                Detected an Active mate

14:30:47 UTC Nov 11 2017
Sync Config                Sync File System           Detected an Active mate

14:30:47 UTC Nov 11 2017
Sync File System           Bulk Sync                  Detected an Active mate

14:31:00 UTC Nov 11 2017
Bulk Sync                  Standby Ready              Detected an Active mate

14:31:39 UTC Nov 11 2017
Standby Ready              Failed                     Interface check
                                                      This host:1
                                                      single_vf: OUTSIDE
                                                      Other host:0

14:31:46 UTC Nov 11 2017
Failed                     Standby Ready              Interface check
                                                      This host:0
                                                      Other host:0

14:33:36 UTC Nov 11 2017
Standby Ready              Just Active                HELLO not heard from mate

14:33:36 UTC Nov 11 2017
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 a sample output from the **show failover history** command on the secondary unit:

```
> show failover history
==========================================================================
From State                To State                  Reason
==========================================================================
17:17:29 UTC Nov 10 2017
Not Detected              Negotiation               No Error

17:18:06 UTC Nov 10 2017
Negotiation               Cold Standby              Detected an Active mate

17:18:08 UTC Nov 10 2017
Cold Standby              Sync Config               Detected an Active mate

17:18:17 UTC Nov 10 2017
Sync Config               Sync File System          Detected an Active mate

17:18:17 UTC Nov 10 2017
Sync File System          Bulk Sync                 Detected an Active mate

17:18:30 UTC Nov 10 2017
Bulk Sync                 Standby Ready             Detected an Active mate

17:19:09 UTC Nov 10 2017
Standby Ready             Failed                    Interface check
                                                    This host:1
                                                    single_vf: OUTSIDE
                                                    Other host:0

17:19:21 UTC Nov 10 2017
Failed                    Standby Ready             Interface check
                                                    This host:0
                                                    Other host:0

==========================================================================
```

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 a sample output from the **show failover history details** command:

```
>show failover history details
==========================================================================
From State                To State                  Reason
==========================================================================
09:58:07 UTC Jan 18 2017
Not Detected              Negotiation               No Error

09:58:10 UTC Jan 18 2017
Negotiation               Just Active               No Active unit found

09:58:10 UTC Jan 18 2017
Just Active               Active Drain              No Active unit found

09:58:10 UTC Jan 18 2017
Active Drain              Active Applying Config    No Active unit found
```

```
09:58:10 UTC Jan 18 2017
Active Applying Config    Active Config Applied       No Active unit found

09:58:10 UTC Jan 18 2017
Active Config Applied     Active                      No Active unit found

================================================================================

PEER History Collected at 09:58:54 UTC Jan 18 2017
=======================PEER-HISTORY=========================================
From State                To State                    Reason
=======================PEER-HISTORY=========================================
09:57:46 UTC Jan 18 2017
Not Detected              Negotiation                 No Error

09:58:19 UTC Jan 18 2017
Negotiation               Cold Standby                Detected an Active mate

09:58:21 UTC Jan 18 2017
Cold Standby             Sync Config                  Detected an Active mate

09:58:29 UTC Jan 18 2017
Sync Config             Sync File System             Detected an Active mate

09:58:29 UTC Jan 18 2017
Sync File System        Bulk Sync                    Detected an Active mate

09:58:42 UTC Jan 18 2017
Bulk Sync               Standby Ready                Detected an Active mate

=======================PEER-HISTORY=========================================
```

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 10: Failover States

States	Description
Disabled	Failover is disabled. This is a stable state.
Failed	The unit is in the failed state. This is a stable state.
Negotiation	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.
Not Detected	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.
Standby Unit States	

States	Description
Cold Standby	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.
Sync Config	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.
Sync File System	The unit synchronizes the file system with the peer unit. This is a transient state.
Bulk Sync	The unit receives state information from the peer. This state only occurs when Stateful Failover is enabled. This is a transient state.
Standby Ready	The unit is ready to take over if the active unit fails. This is a stable state.
Active Unit States	
Just Active	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.
Active Drain	Queues messages from the peer are discarded. This is a transient state.
Active Applying Config	The unit is applying the system configuration. This is a transient state.
Active Config Applied	The unit has finished applying the system configuration. This is a transient state.
Active	The unit is active and processing traffic. This is a stable state.

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 a 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
```

The following is a sample output from the **show failover details** command from peer device on a high-availability pair:

```
> show failover details
        Failover On
Failover unit Secondary
Failover LAN Interface: HA-LINK GigabitEthernet0/3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
1 Hold Interval Success: 12 Failure: 0
2 Hold Interval Success: 15 Failure: 0
3 Hold Interval Success: 15 Failure: 0
4 Hold Interval Success: 15 Failure: 0
5 Hold Interval Success: 15 Failure: 0
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 311 maximum
Interface: management
        1 Hold Success: 0 Failure: 0
        2 Hold Success: 0 Failure: 0
        3 Hold Success: 0 Failure: 0
        4 Hold Success: 0 Failure: 0
        5 Hold Success: 0 Failure: 0
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 99.16(2)10, Mate 99.16(2)10
Serial Number: Ours 9A7WJNE35T5, Mate 9A3497TXPU6
Last Failover at: 06:56:25 UTC Jan 25 2021
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASAv hw/sw rev (/99.16(2)10) status (Up Sys)
                  Interface management (203.0.113.130/fe80::250:56ff:feb7:4927): Unknown
(Waiting)
                slot 1: snort rev (1.0)  status (up)
                snort poll success:2877 miss:0
                slot 2: diskstatus rev (1.0)  status (up)

                disk poll success:2877 miss:0
        Other host: Primary - Active
                Active time: 2910 (sec)
                  Interface management (203.0.113.130): Unknown (Waiting)
                slot 1: snort rev (1.0)  status (up)
                peer snort poll success:2877 miss:0
                slot 2: diskstatus rev (1.0)  status (up)

                peer disk poll success:2877 miss:0

Stateful Failover Logical Update Statistics
        Link : HA-LINK GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         379        0          380        0
        sys cmd         379        0          379        0
        up time         0          0          0          0
        RPC 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    0          0          1          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
```

The following is a sample failover warnings output from the **show failover trace** command:

```
> show failover trace warning
        Warning:Output can be huge. Displaying in pager mode
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer has  1  down ifcs
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer has  1  down ifcs
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
```

The following is sample failover output from the **show failover statistics** command for Versions prior to 7.2.x:

```
ciscoftd(config)# show failover statistics
        tx:121456
        rx:121306
```

The following is sample failover output from the **show failover statistics** command for Version 7.2.x or later:

```
ciscoftd(config)# show failover statistics
        tx:3396
        rx:3296

        Unknown version count for Fover ctl client: 0
        Unknown reason count for peer's switch reason: 0
        fover cd log create failed: 0
```

- The tx and rx counters includes all the **failover control packets**, which are sent or received over the failover LAN interface.
- The "Unknown version count for Fover ctl client" counter is incremented when the **failover control packets** has version as 0 in the received packets.
- The "Unknown reason count for peer's switch reason" counter is incremented if **the received HA switchover reason from peer unit is out of the locally known reason list**.
- The “fover cd log create failed” is set to 1 if the fover cd log file handle was not created.

Related Commands

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

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

active	Displays the **failover exec** command mode for the active unit.
mate	Displays the **failover exec** command mode for the peer unit.
standby	Displays the **failover exec** command mode for the standby unit.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **failover exec** command creates a session with the specified device. By default, that session is in global configuration mode, even though threat defense does not support CLI configuration. The mode information is not relevant for 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

Command	Description
failover exec	Executes the supplied command on the designated unit in a failover pair.

show file

To display information about the file system, use the **show file** command.

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

Syntax Description

descriptors	Displays all open file descriptors.
information *filename*	Displays information about the specified file, including partner application package files.
system	Displays the size, bytes available, type of media, flags, and prefix information about the disk file system.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show file system** command.

```
> show file system
File Systems:
     Size(b)     Free(b)      Type      Flags  Prefixes
* 7935832064    7828107264    disk      rw      disk0: flash:
             -             -  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

Command	Description
dir	Displays the directory contents.
pwd	Displays the current working directory.

show firewall

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

show firewall

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show firewall
Firewall mode: Router
```

Related Commands

Command	Description
configure firewall	Sets the firewall mode.
show mode	Shows the current context mode, either single or multiple.

show flash

To display the contents of the internal Flash memory, use the **show flash:** command.

show flash: [**all** | **controller** | **filesys**]

Note In threat defense, the **flash** keyword is aliased to **disk0**.

Syntax Description

all	Displays all Flash information.
controller	Displays file system controller information.
filesys	Displays file system information.

Command History

Release	Modification
6.1	This command was introduced.

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

Command	Description
dir	Displays the directory contents.
show disk0:	Displays the contents of the internal Flash memory.
show disk1:	Displays the contents of the external Flash memory card.

show flow-export counters

To view the runtime counters for NetFlow statistical and error data, use the **show flow-export counters** command.

show flow-export counters

Command History

Release	Modification
6.3	This command was introduced.

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

Command	Description
clear flow-export counters	Resets all runtime counters in NetFlow to zero.

show flow-offload

To view flows, counters, statistics, and information about offloaded flows, use the **show flow-offload** command.

This command is available on threat defense on the Firepower 4100/9300 chassis.

show flow-offload {**flow** [**count** | **detail**] | **dynamic** [**count** | **detail**] | **static** [**count** | **detail**] | **info** [**detail**] | **statistics**}

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

Release	Modification
6.3	This command was introduced.

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. Offloaded flows are identified by an index number, which is calculated by hashing the source and destination IP addresses, ports, and the protocol. A *collision* occurs when the system tries to offload a flow that has the same index as a currently active offloaded flow. In this case, the new flow is not offloaded, but the first flow remains offloaded.

```
>show flow-offload flow
Total offloaded flow stats: 4 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
    rw(0): cmd '  replace', offset  0, bytes 12, data(x) 90E2 BA01 8E29 B0AA 7730 097B
    rw(1): cmd 'increment', offset 46, bytes  4, data(x) 422AC658
```

Following is example output from the **show flow-offload dynamic** command.

```
>show flow-offload flow 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.

```
>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.

```
>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 630342730
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.

```
>show flow-offload flow 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.

```
> show flow-offload flow 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.

```
> 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

Commands	Description
configure flow-offload	Enable or disable dynamic flow offload.
clear flow-offload	Clears dynamic flow offload counters or statistics.

show flow-offload-ipsec

To display information about IP sec flow off-loading, use the **show flow-offload-ipsec**.

show flow-offload-ipsec { **info** | **option-table** | **statistics** }

Syntax Description

info	Show information about the current configuration state for IPsec flow offload.
option-table	Show table information for the content addressable memory (CAM) used in IPsec flow offload. This information is for debugging only and it is not meaningful to an end user.
statistics	Show content addressable memory (CAM) statistics for the offloaded flows.

Command History

Release	Modification
7.2	This command was introduced.

Example

The following example shows the current configuration state of IPsec flow offload.

```
ciscoasa# show flow-offload-ipsec info
IPSec offload : Enabled
Egress optimization: Enabled
```

The following example shows statistics.

```
> show flow-offload-ipsec statistics

        Packet stats of Pipe 0
        ----------------------
        Rx Packet count                          :               0
        Tx Packet count                          :               0
        Error Packet count                       :               0
        Drop Packet count                        :               0

        CAM stats of Pipe 0
        ----------------------
        Option ID Table CAM Hit Count            :              38
        Option ID Table CAM Miss Count           :             154
        Tunnel Table CAM Hit Count               :               0
        Tunnel Table CAM Miss Count              :               0
        6-Tuple CAM Hit Count                    :               0
        6-Tuple CAM Miss Count                   :              38
```

The following example shows the option table.

```
> show flow-offload-ipsec option-table
        instance_id:256 interface_id:124 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:123 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:122 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:121 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:120 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:119 action:0 logic_id_opt:0 subinterface_id_opt:0
```

```
instance_id:256 interface_id:118 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:117 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:156 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:157 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:158 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:159 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:112 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:111 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:110 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:109 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:108 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:107 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:106 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:105 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:104 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:103 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:102 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:101 action:0 logic_id_opt:0 subinterface_id_opt:0
```

Related Commands

Command	Description
clear flow-offload-ipsec	Clears IPsec flow offload statistics.

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

id [*fqdn_id*]	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.
	
	`object network www.example.com`
	` fqdn www.example.com id 1001`

ip [*ip_address*]	Displays information based on the IP address obtained from the DNS server. You can optionally enter an IP address.

Command History

Release	Modification
6.3	This command was introduced.

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

Command	Description
clear dns	Removes FQDN network object DNS resolutions.
show dns	Displays FQDN network object DNS resolutions.
show running-config	Displays the running configuration.

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 threat defense interface.

Command Default

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

Command History

Release	Modification
6.1	This command was introduced.
6.7	The output for the **show fragment** command was enhanced to include IP fragment related drops and error counters.

Examples

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

```
> show fragment
Interface: inside
Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
Run-time stats: Queue: 0, Full assembly: 12
Drops: Size overflow: 0, Timeout: 0,
Chain overflow: 0, Fragment queue threshold exceeded: 0,
Small fragments: 0, Invalid IP len: 0,
Reassembly overlap: 26595, Fraghead alloc failed: 0,
SGT mismatch: 0, Block alloc failed: 0,
Invalid IPV6 header: 0
```

Where:

- Size: The maximum number of blocks that are allowed to reside in fragment database (per interface) at any given point that you had configured as default.
- Chain: The maximum number of fragments into which a full IP packet can be fragmented. The default is 24.
- Timeout: The maximum number of seconds to wait for an entire fragmented packet to arrive. The default is 5 seconds.
- Reassembly: virtual or full. The default is virtual reassembly. IP fragments that terminate at the ASA or require inspection at the application level are fully (physically) reassembled. The packet that was fully (physically) reassembled can be fragmented again on the egress interface, if necessary.
- Size Overflow: The maximum number of blocks that are allowed to reside in fragment database at any given point has reached. The overflow counter measures the drops due to reaching the default size for fragment data base. This counter does not include the number of fragments that are dropped because of queue size (2/3 of the max DB size).

- Timeout: The fragment chain timed out before the reassembly was completed.
- Chain limit: The individual fragment chain limit has reached.
- Fragment queue threshold exceeded: The fragment database threshold, that is 2/3 of the queue size per interface, has exceeded.
- Small fragments: When fragment offset is greater than 0 but less than 16.
- Invalid packet len: Invalid IP packet length (for example, len > 65535).
- Reassembly overlap: Duplicate or overlapping fragments were detected.
- Fraghead alloc failed: Failed to allocate fragment head. Fraghead maintains the chain of all fragments for an IP packet.
- SGT mismatch: SGT value did not match among fragments of the same IP packets.
- Block alloc failed: Allocation failed for full reassembly.
- Invalid IPV6 header: Encountered invalid IPV6 header during full reassembly.

Related Commands

Command	Description
clear configure fragment	Clears the IP fragment reassembly configuration and resets the defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

show gc

To display the garbage collection process statistics, use the **show gc** command.

show gc

Command History

Release	Modification
6.1	This command was introduced.

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

Command	Description
clear gc	Removes the garbage collection process statistics.

show h225

To display information for H.225 sessions established across the threat defense device, use the **show h225** command.

show h225

Command History

Release	Modification
6.1	This command was introduced.

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
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
    Local:   10.130.56.4/1050   Foreign: 172.30.254.205/1720
```

This output indicates that there is currently 1 active H.323 call going through the 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.

Related Commands

Commands	Description
show h245	Displays information for H.245 sessions established across the device by endpoints using slow start.
show h323 ras	Displays information for H.323 RAS sessions established across the device.

show h245

To display information for H.245 sessions established across the threat defense device by endpoints using slow start, use the **show h245** command.

show h245

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show h245** command displays information for H.245 sessions established across the 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
1       10.130.56.3/1041        0       172.30.254.203/1245    0
        MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
                       Local   10.130.56.3 RTP 49608 RTCP 49609
        MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
                       Local   10.130.56.3 RTP 49606 RTCP 49607
```

There is currently one H.245 control session active across the 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

Commands	Description
show h245	Displays information for H.245 sessions established across the threat defense device by endpoints using slow start.

Commands	Description
show h323 ras	Displays information for H.323 RAS sessions established across the threat defense device.

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 threat defense device between a gatekeeper and its H.323 endpoint.
gup	Displays information about the H323 gateway updated protocol connections.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show h323 ras** command displays information for H.323 RAS sessions established across the 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

Commands	Description
show h245	Displays information for H.245 sessions established across the threat defense device by endpoints using slow start.

show hardware-bypass

To display the current hardware bypass status on an ISA 3000, use the **show hardware-bypass** command.

show hardware-bypass

Command History

Release	Modification
6.3	This command was introduced.

Examples

The following is sample output from the **show hardware-bypass** command.

```
> show hardware-bypass
                          Status              Powerdown           Powerup
GigabitEthernet 1/1-1/2   Disable             Disable             Disable
GigabitEthernet 1/3-1/4   Disable             Disable             Disable

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

Release	Modification
6.1	This command was introduced.

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.

```
> 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 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
        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
```

```
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

Logical Update Queue Information
                Cur     Max     Total
Recv Q:         0       10      234
Xmit Q:         0       11      1200
```

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.

```
> 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
```

Related Commands

Commands	Description
show failover	Shows the failover (high-availability) configuration.

show https-access-list

The **show https-access-list** command displays the HTTPS access lists configured on the device.

show https-access-list

Command History

Release	Modification
6.1	This command was introduced.

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, 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

Commands	Description
configure https-access-list	Configures the HTTPS access list on the management interface.