

show f – show ipu

- show facility-alarm, on page 3
- show failover, on page 6
- show failover descriptor, on page 26
- show failover exec, on page 27
- show failover config-sync, on page 29
- show fault-monitor block-depletion, on page 35
- show fault-monitor mbuf-depletion, on page 37
- show file, on page 38
- show fips, on page 41
- show firewall, on page 43
- show flash, on page 44
- show flow-export counters, on page 46
- show flow-offload, on page 48
- show flow-offload-ipsec, on page 52
- show fragment, on page 54
- show fxos mode, on page 56
- show gc, on page 58
- show h225, on page 59
- show h245, on page 61
- show h323, on page 63
- show hardware-bypass, on page 65
- show history, on page 66
- show hostname, on page 68
- show icmp, on page 69
- show idb, on page 70
- show igmp groups, on page 72
- show igmp interface, on page 74
- show igmp traffic, on page 75
- show import webvpn, on page 76
- show interface, on page 78
- show interface ip brief, on page 93
- show inventory, on page 96
- show ip address, on page 100

- show ip address dhcp, on page 102
- show ip address pppoe, on page 106
- show ip audit count, on page 108
- show ip local pool, on page 110
- show ip verify statistics, on page 111
- show ips, on page 112
- show ipsec df-bit, on page 114
- show crypto ipsec fragmentation, on page 116
- show ipsec policy, on page 118
- show ipsec sa, on page 120
- show ipsec sa summary, on page 128
- show ipsec stats, on page 130

show facility-alarm

To display the triggered alarms in an ISA 3000 device, use the **show facility-alarm** command in user EXEC mode.

show facility-alarm { **relay | status** [**info | major | minor**] }

Syntax Description

relay	Displays the alarms that have energized the alarm output relay.
status [**info** | **major** | **minor**]	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 Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

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.

Column	Description
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:

```
ciscoasa> show facility-alarm relay

Source    Severity   Description                          Relay      Time
ciscoasa  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:

```
ciscoasa> show facility-alarm status info

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

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.
alarm contact severity	Specifies the severity of alarms.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.

Command	Description
alarm facility power-supply rps	Configures the power supply alarms.
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays the status of the input alarm contacts.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

show failover

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

show failover [**descriptor**] [**exec**] [**group** *num* | **history** [**details**] | **interface** | **state** | **trace** [*options*] | [**statistics** [**all** | **events** | **unit** | **np-clients** | **cp-clients** | **bulk-sync** [**all** | **control-plane** | **data-plane** |] | **interface** [**all**]] | **details**] [**config-sync**]

Syntax Description

descriptor	Shows failover interface descriptors in the form of two numbers for every interface. When exchanging information about an interface, this unit uses the first number in the messages it sends to its peer. And it expects the second number in the messages it receives from its peer.
details	Displays the failover details of the pairs in a high availability pair.
exec	Shows failover command execution information.
group	Displays the running state of the specified failover group.
history [details]	Displays failover history. The failover history displays past failover state changes and the reason for the state change for the active unit. The failover history includes the failure reason along with its specific details; this helps with troubleshooting. Add the details keyword to display failover history from the peer unit. This includes failover state changes and the reason for the state change, for the peer unit. History information is cleared when the device reboots.
interface	Displays failover and stateful link information.
num	Failover group number.
state	Displays the failover state of both the failover units. The information displayed includes the primary or secondary status of the unit, the Active/Standby status of the unit, and the last reported reason for failover. The fail reason remains in the output even when the reason for failure is cleared.

trace [*options*]	(Optional) Shows the failover event trace. Options include to show the failover event trace by levels (1-6): • **critical** — to filter failover critical event trace (level = 1) • **debugging**— to filter failover debugging trace (Debug level = 6) • **error**— to filter failover internal exception (level = 2) • **informational**— to filter failover informational trace (level = 5) • **notice**— to filter failover notices (level = 4) • **warning**— to filter failover warnings (level = 3)
statistics [**all** | **events** | **unit** | **np-clients** | **cp-clients** | **bulk-sync** [**all** | **control-plane** | **data-plane**	Displays local device events, transmit, and receive packet counts of failover interface and bulk-sync time duration • **np-clients**—displays the HA data-path client's packet's statistics. • **cp-clients**—displays the HA control plane client's packet's statistics. • **bulk-sync**—displays the sync time for the HA data-plane clients and control-plane clients, or both. • **events**—displays the local failures notified by App agent—HA LAN link uptime, Supervisor's heartbeat failures, and Disk full issues. • **all**—displays the consolidated failover statistics for interface, np-client, cp-client, and bulk-sync.
details	Displays the failover details of the pairs in a high availability pair.
config-sync	Displays device configuration, device status, and checksum details about the Config-Sync Optimization feature.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.1(6)	The **details** keyword was added.
7.0(1)	This command was modified. The output includes additional information.
8.2(2)	This command was modified. The output includes IPv6 addresses for firewall and failover interfaces. The Stateful Failover statistics output includes information for the IPv6 neighbor discover table (IPv6 ND tbl) updates.
9.9.2	This command was modified. The failover history output includes enhancements to the failure reasons. The history details keyword was added. This displays failover history from the peer unit.
9.16(1)	The **details** keyword was added
9.18(1)	The **config-sync** keyword was added.
9.20(2)	The **statistics all**,**statistics events**,**statistics np-clients**,**statistics cp-clients**, and **statistics bulk-sync** keywords were 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.



Note Stateful Failover, and therefore Stateful Failover statistics output, is not available on the ASA 5505.

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 ASA up time, which the active ASA passes on to the standby ASA.

- 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

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.

Table 7-1 describes the interface states for failover.

Table 1: 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.

State	Description
Link Down	The physical link is up, but the interface is administratively down.
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 (using the **no shutdown** command in interface configuration mode), 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.

Usage Guidelines

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

Examples

The following is a sample output from the **show failover** command for Active/Standby Failover. The ASAs use IPv6 addresses on the failover link (folink) and the inside interface.

```
ciscoasa# show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/4 (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 1049 maximum
MAC Address Move Notification Interval not set
Version: Ours 98.1(1)86, Mate 98.1(1)86
Serial Number: Ours JAF1610APKQ, Mate JAF1610ALGM
Last Failover at: 12:52:34 UTC Apr 26 2017
        This host: Primary - Active
                Active time: 87 (sec)
                slot 0: ASA5585-SSP-10 hw/sw rev (2.0/98.1(1)86) status (Up Sys)
                  Interface inside (10.86.118.1): Normal (Monitored)
                  Interface outside (192.168.77.1): No Link (Waiting)
                  Interface dmz (192.168.67.1): No Link (Waiting)
                slot 1: empty
                slot 1: empty
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5585-SSP-10 hw/sw rev (2.0/98.1(1)86) status (Up Sys)
                  Interface inside (10.86.118.2): Normal (Waiting)
                  Interface outside (192.168.77.2): No Link (Waiting)
                  Interface dmz (192.168.67.2): No Link (Waiting)
                slot 1: empty
                slot 1: empty
Stateful Failover Logical Update Statistics
```

```
Link : failover GigabitEthernet0/4 (up)
Stateful Obj    xmit       xerr       rcv        rerr
General         22         0          6          0
sys cmd         6          0          6          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         14         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       1          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       5       6
Xmit Q:         0       27      86
```

The following is a sample output from the **show failover** command for Active/Active Failover. In this example, only the admin context has IPv6 addresses assigned to the interfaces.

```
ciscoasa# show failover
Failover On
Failover unit Primary
Failover LAN Interface: folink GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004
  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)
                slot 0: ASA-5545 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                admin Interface outside (10.132.8.5): Normal
                admin Interface folink (10.132.9.5/fe80::2a0:c9ff:fe03:101): Normal
                admin Interface inside (10.130.8.5/fe80::2a0:c9ff:fe01:101): Normal
                admin Interface fourth (10.130.9.5/fe80::3eff:fe11:6670): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal
  Other host:   Secondary
```

```
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)
                slot 0: ASA-5545 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                admin Interface outside (10.132.8.6): Normal
                admin Interface folink (10.132.9.6/fe80::2a0:c9ff:fe03:102): Normal
                admin Interface inside (10.130.8.6/fe80::2a0:c9ff:fe01:102): Normal
                admin Interface fourth (10.130.9.6/fe80::3eff:fe11:6671): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal
Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     22         0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
  SIP Session    0          0          0          0
        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

The following is a sample output from the **show failover** command on the ASA 5505:

```
Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan150 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(0)55, Mate 7.2(0)55
Last Failover at: 19:59:58 PST Apr 6 2006
        This host: Primary - Active
                Active time: 34 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.1): Normal
                  Interface outside (192.168.2.201): Normal
                  Interface dmz (172.16.0.1): Normal
                  Interface test (172.23.62.138): Normal
                slot 1: empty
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.2): Normal
                  Interface outside (192.168.2.211): Normal
                  Interface dmz (172.16.0.2): Normal
                  Interface test (172.23.62.137): Normal
                slot 1: empty
```

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

```
ciscoasa(config)# show failover state
               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
    Group 2    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
Other host -   Primary
    Group 1    Active         Comm Failure             03:41:12 UTC Apr 17 2009
    Group 2    Active         Comm Failure             03:41:12 UTC Apr 17 2009
====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

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

```
ciscoasa(config)# show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             12:53:10 UTC Apr 26 2017
====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

The following is a sample output from the **show failover state** command for an active-standby setup, where the configurations match in both units:

```
firepower(config)# show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             10:24:54 UTC May 9 2023
====Configuration State===
        Sync Skipped
====Communication State===
        Mac set
```

Table 7-2 describes the output of the **show failover state** command.

Table 2: show failover state Output Description

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. • **Sync Skipped - STANDBY**—Set when the configurations in the standby unit and active unit match and no configuration synchronization is done 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. • **Sync Skipped**—Set when the configurations in the active unit and standby unit match and no configuration synchronization occurs on 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**

Field	Description
State	Displays the Primary/Secondary and Active/Standby status for the unit.
This host/Other host	This host indicates information for the device upon which the command was executed. Other host indicates information for the other device in the failover pair.

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

```
ciscoasa(config)# show failover history
==============================================
From State                 To State                   Reason
==============================================
11:59:31 UTC Jan 13 2017
Active Config Applied      Active                     No Active unit found

06:17:51 UTC Jan 15 2017
Active                     Failed                     Interface check
                                                        This Host:3
                                                          admin: inside
                                                          ctx-1: ctx1-1
                                                          ctx-2: ctx2-1
                                                        Other Host:0
03:58:49 UTC Feb 3 2017
Active                     Cold Standby               Failover state check delayed due to
 mate failure

03:58:51 UTC Feb 3 2017
Cold Standby               Sync Config                Failover state check delayed due to
 mate failure

03:59:18 UTC Feb 3 2017
Sync Config                Sync File System           Failover state check delayed due to
 mate failure
23:11:39 UTC Jan 13 2017
Cold Standby              Failed                    HA state progression failed as response
 not heard from mate

23:19:01 UTC Jan 13 2017
Sync Config                Not Detected               HA state progression failed as
configuration sync timeout expired
 14:26:28 UTC Aug 16 2017
Standby Ready              Just Active                Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Just Active                Active Drain               Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Drain               Active Applying Config     Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Applying Config     Active Config Applied      Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Config Applied      Active                     Inspection engine in other unit has
failed due to disk failure

18:03:35 UTC Aug 17 2017
```

```
Active                    Standby Ready             Other unit wants me Standby

18:03:36 UTC Aug 17 2017
Standby Ready             Failed                    Detect Inspection engine failure due
 to disk failure

18:03:37 UTC Aug 17 2017
Failed                    Standby Ready             My Inspection engine is as good as
peer due to disk recovery
```

Each entry provides the time and date the state change occurred, the beginning state, the resulting state, and the reason for the state change. The newest entries are located at the bottom of the display. Older entries appear at the top. A maximum of 60 entries can be displayed. Once the maximum number of entries has been reached, the oldest entries are removed from the top of the output as new entries are added to the bottom.

The failure reasons include details that help in troubleshooting. These include interface check, failover state check, state progression failure and service module failure.

The following is sample output from the show failover history details command:

```
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.

Table 7-3 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 3: 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	
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 sample output from the **show failover interface** command. The device has an IPv6 address configured on the failover interface.

```
ciscoasa(config)# 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 sample failover warnings output from the **show failover trace** command:

```
ciscoasa(config)# 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 Version prior to 9.18:

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

The following is sample failover output from the **show failover statistics** command for Version 9.18 or later:

```
ciscoasa(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 locally known reason list**.

The “fover cd log create failed” is set to 1 if the fover cd log file handle was not created.

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

```
ciscoasa(config)# show failover statistics all

show failover statistics unit
-----------------------------
Unit Poll frequency 2 seconds, holdtime 10 seconds
Failover unit health statistics set size 10
1 Hold Interval Success: 3 Failure: 0
2 Hold Interval Success: 5 Failure: 0
3 Hold Interval Success: 5 Failure: 0
4 Hold Interval Success: 5 Failure: 0
5 Hold Interval Success: 5 Failure: 0

show failover statistics interface all
--------------------------------------
Interface Poll frequency 2 seconds, holdtime 10 seconds
Interface Policy 1
Monitored Interfaces 3 of 1285 maximum
Health statistics monitored interfaces 3
Failover interface health statistics set size 10
Interface: outside
 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
Interface: inside
 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
Interface: diagnostic
 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

show failover statistics np-clients
-----------------------------------

Abbreviations:
BLErr - Buffer lock error, HIErr - HA Interface error, PI - Peer incompatible
PSErr - Packet size error, IPkt - Invalid pkt, CPkt - Corrupted pkt
BErr - Buffer error, MDErr - Msg descriptor error, MxBErr - Multiplexer buffer error
MxBDErr - Multiplexer buffer descriptor error

HA DP Clients Statistics

TX Statistics
-------------------------------------------------------------------------------------------------------
Client Name                                    Tx In        Tx Out       BLErr        HIErr
        PI
-------------------------------------------------------------------------------------------------------
SNP HA private client                             0            0            0            0
            0
Soft NP flow stateful failover                    0            0            0            0
            0
Soft NP SVC stateful failover                     0            0            0            0
```

```
            0
SIP inspection engine                          0           0           0           0
            0
SCTP inspection engine                         0           0           0           0
            0
Soft NP NLP HA client                          16          16          0           0
            0
ODNS inspection engine                         0           0           0           0
            0
DNS BRANCH/SNOOPING module                     0           0           0           0
            0
ARP DP module                                  0           0           0           0
            0
TFW DP module                                  0           0           0           0
            0
SNP HA Heartbeat client                        1130        1130        0           0
            0
ZTNA DP module                                 0           0           0           0
            0
Unknown client                                 0           0           0           0
            0

RX Statistics
-------------------------------------------------------------------------------------------------------------
Client Name                                    Rx In       Rx Out      PSErr
IPkt         CPkt         PI
-------------------------------------------------------------------------------------------------------------
SNP HA private client                            0           0           0
 0           0            0
Soft NP flow stateful failover                   0           0           0
 0           0            0
Soft NP SVC stateful failover                    0           0           0
 0           0            0
SIP inspection engine                            0           0           0
 0           0            0
SCTP inspection engine                           0           0           0
 0           0            0
Soft NP NLP HA client                            1           1           0
 0           0            0
ODNS inspection engine                           0           0           0
 0           0            0
DNS BRANCH/SNOOPING module                       0           0           0
 0           0            0
ARP DP module                                    0           0           0
 0           0            0
TFW DP module                                    0           0           0
 0           0            0
SNP HA Heartbeat client                          1121        1121        0
 0           0            0
ZTNA DP module                                   0           0           0
 0           0            0
Unknown client                                   0           0           0
 0           0            0

Buffer Failure Statistics
-------------------------------------------------------------------------------------------------------------
Client Name                                  BErr        MDErr       MxBErr
MxBDErr
-------------------------------------------------------------------------------------------------------------
SNP HA private client                          0           0           0           0

Soft NP flow stateful failover                 0           0           0           0

Soft NP SVC stateful failover                  0           0           0           0
```

```
SIP inspection engine                          0           0           0           0
SCTP inspection engine                         0           0           0           0
Soft NP NLP HA client                          0           0           0           0
ODNS inspection engine                         0           0           0           0
DNS BRANCH/SNOOPING module                     0           0           0           0
ARP DP module                                  0           0           0           0
TFW DP module                                  0           0           0           0
SNP HA Heartbeat client                        0           0           0           0
ZTNA DP module                                 0           0           0           0
Unknown client                                 0           0           0           0
-------------------------------------------------------------------------------------------------------

show failover statistics bulk-sync
----------------------------------


For session 0, NP Client Bulk Sync stats
=================================================================================================

 Client Name                          Status              Start Time                  End
Time         Time Taken
=================================================================================================

 Soft NP flow stateful failover       Done          06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 Soft NP SVC stateful failover        Done          06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 SCTP inspection engine               Done          06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 DNS BRANCH/SNOOPING module           Done          06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 ARP DP module                        Done          06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 TFW DP module                        Done          06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 ZTNA DP module                       Done          06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
=================================================================================================


For session 0, CP Client Bulk Sync stats
=================================================================================================

 Client Name                                    Status                Start Time
       End Time          Time Taken
=================================================================================================

 HA Internal Control                            Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Failover Control Module                        Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Legacy LU support                              Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
```

```
 vpnfo                                           Done          06:44:50 UTC Feb 10 2023
06:45:00 UTC Feb 10 2023   00:00:10
 vpnfo                                           Done          06:44:50 UTC Feb 10 2023
06:45:00 UTC Feb 10 2023   00:00:10
 SIP inspection engine                           Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 NetFlow Module                                  Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 HA Shared License Client                        Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Route HA engine                                 Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 CTS                                             Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 CTS SXP Module                                  Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 IPv6 Route HA engine                            Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Service Tag Switching Module                    Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 CFG_HIST HA Client                              Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 SCTP inspection engine                          Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 KCD                                             Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 HA CD Proxy Client                              Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 DHCPv6 HA engine                                Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Attribute Module                                Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 ODNS inspection engine                          Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Ruld ID DB Client                               Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 DNS branch HA CP client                         Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 DNS_TRUSTED_SOURCE module                       Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Threat-Detection                                Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 ZTNA HA Module                                  Done          06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
```

```
Failover cumulative packet statistics
-------------------------------------
    tx:854
    rx:786
```

The following is a sample output (only non-zero rows) from the **show failover statistics cp-clients** command:

```
show failover statistics cp-clients

Abbreviations:
TxIn - Pkt rcvd at HA from client, TxOut - Pkt sent from HA to Interface
BErr - Buffer alloc failure, MDErr - Msg desc alloc failure, AckRcvd - Ack rcvd
ReTx - Retransmit pkts, NoSvc - HA service is down, PIErr - Client is incompatible
EncErr - Error in encrypting pkt, RepCfg - Replace cfg enabled
RxIn - Pkt rcvd from Interface to HA, RxOut - Pkt sent from HA to client
MDErr - Msg desc alloc failure, AckSent - Ack sent, NMsgCb - No Msg callback for client
InVcid - Invalid vcid rcvd, PIErr - Client is incompatible, InvPkt - Invalid pkt rcvd,
```

```
HA CP Clients Statistics

TX Statistics
-----------------------------------------------------------------------------------------------------------
Client Name                    TxIn          TxOut       BErr   MDErr  AckRcvd       ReTx
  NoSvc  PIErr  EncErr RepCfg
-----------------------------------------------------------------------------------------------------------
Legacy LU Support  478  478 0 0 0  0 0 0 0 0
vpnfo    2  2   0 0 2  0 0 0 0 0
HA CD Proxy Client  17  17  0 0 17       0 0 0 0 0
-----------------------------------------------------------------------------------------------------------
Total Aggressive Ack rcvd      :   0

RX Statistics
-----------------------------------------------------------------------------------------------------------
Client Name                    RxIn          RxOut         MDErr  AckSent       NMsgCb
InVcid PIErr  InvPkt
-----------------------------------------------------------------------------------------------------------
Legacy LU Support  478  478  0 0  0 0 0 0
vpnfo        1960     1960   0 12  0 0 0 0
CTS    1  1      0 1  0 0 0 0
CFG_HIST HA Client  12  12   0 12  0 0 0 0
HA CD Proxy Client  10  10   0 10  0 0 0 0
ZTNA HA Module      1   1    0 1   0 0 0 0
-----------------------------------------------------------------------------------------------------------
Total Aggressive Ack sent        :   0
Total Invalid pkts rcvd          :   0
Total unknown client pkts rcvd   :   0
```

The following is a sample output (only non-zero rows) from the **show failover statistics np-clients** command:

```
show failover statistics np-clients

Abbreviations:
BLErr - Buffer lock error, HIErr - HA Interface error, PI - Peer incompatible
PSErr - Packet size error, IPkt - Invalid pkt, CPkt - Corrupted pkt
BErr - Buffer error, MDErr - Msg descriptor error, MxBErr - Multiplexer buffer error
MxBDErr - Multiplexer buffer descriptor error

HA DP Clients Statistics

TX Statistics
-----------------------------------------------------------------------------------------
Client Name                     Tx In          Tx Out       BLErr   HIErr  PI
-----------------------------------------------------------------------------------------
Soft NP flow stateful failover 1420091  1420091 0 0 0
Soft NP NLP HA client    45131    45131   0 0 0
Soft NP NLP HA client current  45129    45129   0 0 0
SNP HA Heartbeat Client  4240     4240    0 0 0
-----------------------------------------------------------------------------------------

RX Statistics
-----------------------------------------------------------------------------------------
Client Name                     Rx In          Rx Out       PSErr   IPkt  CPkt PI
-----------------------------------------------------------------------------------------
Soft NP NLP HA client    7943     7943    0 0 0  0
Soft NP NLP HA client current  7943     7943    0 0 0  0
SNP HA Heartbeat client  4185     4185    0 0 0  0
-----------------------------------------------------------------------------------------
Buffer Failure Statistics
-----------------------------------------------------------------------------------------
Client Name                     BErr          MDErr       MxBErr MxBDErr
-----------------------------------------------------------------------------------------
```

Soft NP NLP HA is the HA client.

Soft NP NLP HA Current shows the counters for app sync in the current session:

- NP = Data plane
- Soft NP = Internal constructs of the data plane
- NLP = Non-Lina processes

The following is a sample output from the **show failover statistics events** command that shows the failover events statistics information:

```
show failover statistics events

Info: Failover Lan interface came UP at 05:01:23 UTC Oct 18 2023
Codes: A -Blade Id, B -Chassis Id C -Re enable failover
======================================================================
MIO Events Table|                Time              A| B | C|
MIO heartbeat recovered| 05:00:52 UTC Oct 18 2023| 1| 0| true|
MIO heartbeat recovered| 05:04:02 UTC Oct 18 2023| 1| 0|false|
```

Related Commands

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

show failover descriptor

Shows failover interface descriptors. It shows two numbers for every interface. When exchanging information about an interface, this unit uses the first number in the messages it sends to its peer. And it expects the second number in the messages it receives from its peer. For troubleshooting, collect the show output from both the units, and verify whether the numbers match.

show failover descriptor

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2	This command was added.

Examples

The following is sample output from the show failover descriptor command.

```
asa# show failover descriptor
outside send:   20100ffff0001  receive:   20100ffff0002
mgmt    send:   10000ffff0001  receive:   10000ffff0002
inside  send: 20001ffffff0001  receive: 20001ffffff0002
```

show failover exec

To display the **failover exec** command mode for the specified unit, use the **show failover exec** command in privileged EXEC mode.

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 Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **failover exec** command creates a session with the specified device. By default, that session is in global configuration mode. You can change the command mode of that session by sending the appropriate command (such as the **interface** command) using the **failover exec** command. Changing **failover exec** command modes for the specified device does not change the command mode for the session you are using to access the device. Changing commands modes for your current session to the device does not affect the command mode used by the **failover exec** command.

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. This example demonstrates that the command mode for the unit where the **failover exec** commands are being entered does not have to be the same as the **failover exec** command mode where the commands are being executed.

In this example, an administrator logged into the standby unit adds a name to an interface on the active unit. The second time the **show failover exec mate** command is entered in this example shows the peer device in interface configuration mode. Commands sent to the device with the **failover exec** command are executed in that mode.

```
ciscoasa(config)# show failover exec mate
Active unit Failover EXEC is at config mode! The following command changes the standby unit
 failover exec mode ! to interface configuration mode.ciscoasa(config)# failover exec mate
 interface GigabitEthernet0/1
ciscoasa(config)# show failover exec mate
Active unit Failover EXEC is at interface sub-command mode! Because the following command
is sent to the active unit, it is replicated ! back to the standby unit.ciscoasa(config)#
failover exec mate nameif test
```

Related Commands

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

show failover config-sync

To display details of the config-sync optimization feature, use the **show failover config-sync** command in privileged EXEC mode.

show failover config-sync { **checksum | configuration | status** }

Syntax Description

checksum	Displays the device status and checksum information.
configuration	Displays the device failover configuration and checksum information.
status	Displays the config-sync optimization status information.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.18.(1)	This command was added.

Usage Guidelines

The **showfailover config-sync** command displays the status of Config Sync Optimization feature, device configuration, and the checksum information. By default, that session is in global configuration mode.

Examples

The following are the sample output from the **showfailoverconfig-synccheckSum** command for the active and standby units.

```
ciscoasa# show failover config-sync checksum
My State: Active
Config Hash: 12daf457c6a1e875a175a67cab7f0c56
```

```
ciscoasa# show failover config-sync checksum
My State: Standby Ready
Config Hash: 12daf457c6a1e875a175a67cab7f0c56
```

The following are the sample output from the **showfailoverconfig-syncconfiguration** command.

```
cicoasa#show failover config-sync configuration
My State: Negotiation
[1]: Cmd_: !
[2]: Cmd_: enable password $sha512$5000$eTI8yiQxuWYEzeypFF6qdw==$HNf7i1tpOugBBnUSIzrlPA==
pbkdf2
[3]: Cmd_: service-module 0 keepalive-timeout 4
[4]: Cmd_: service-module 0 keepalive-counter 6
[5]: Cmd_: !
[6]: Cmd_: license smart
[7]: Cmd_:  feature tier standard
[8]: Cmd_:  throughput level 10G
[9]: Cmd_: names
[10]: Cmd_: no mac-address auto
[11]: Cmd_: !
[12]: Cmd_: interface GigabitEthernet0/0
[13]: Cmd_:  shutdown
[14]: Cmd_:  no nameif
[15]: Cmd_:  no security-level
[16]: Cmd_:  no ip address
[17]: Cmd_: !
[18]: Cmd_: interface GigabitEthernet0/1
[19]: Cmd_:  shutdown
[20]: Cmd_:  no nameif
[21]: Cmd_:  no security-level
[22]: Cmd_:  no ip address
[23]: Cmd_: !
[24]: Cmd_: interface GigabitEthernet0/2
[25]: Cmd_:  shutdown
[26]: Cmd_:  no nameif
[27]: Cmd_:  no security-level
[28]: Cmd_:  no ip address
[29]: Cmd_: !
[30]: Cmd_: interface GigabitEthernet0/3
[31]: Cmd_:  shutdown
[32]: Cmd_:  no nameif
[33]: Cmd_:  no security-level
[34]: Cmd_:  no ip address
[35]: Cmd_: !
[36]: Cmd_: interface GigabitEthernet0/4
[37]: Cmd_:  shutdown
[38]: Cmd_:  no nameif
[39]: Cmd_:  no security-level
[40]: Cmd_:  no ip address
[41]: Cmd_: !
[42]: Cmd_: interface GigabitEthernet0/5
[43]: Cmd_:  shutdown
[44]: Cmd_:  no nameif
[45]: Cmd_:  no security-level
[46]: Cmd_:  no ip address
[47]: Cmd_: !
[48]: Cmd_: interface GigabitEthernet0/6
[49]: Cmd_:  shutdown
[50]: Cmd_:  no nameif
[51]: Cmd_:  no security-level
[52]: Cmd_:  no ip address
[53]: Cmd_: !
[54]: Cmd_: interface GigabitEthernet0/7
[55]: Cmd_:  shutdown
[56]: Cmd_:  no nameif
[57]: Cmd_:  no security-level
[58]: Cmd_:  no ip address
[59]: Cmd_: !
[60]: Cmd_: interface GigabitEthernet0/8
```

```
[61]: Cmd_:  description LAN/STATE Failover Interface
[62]: Cmd_: !
[63]: Cmd_: interface Management0/0
[64]: Cmd_:  no management-only
[65]: Cmd_:  nameif management
[66]: Cmd_:  security-level 0
[67]: Cmd_:  ip address 192.168.2.63 255.255.255.0 standby 192.168.2.64
[68]: Cmd_: !
[69]: Cmd_: ftp mode passive
[70]: Cmd_: no object-group-search access-control
[71]: Cmd_: pager lines 23
[72]: Cmd_: mtu management 1500
[73]: Cmd_: failover
[74]: Cmd_: failover lan interface fover GigabitEthernet0/8
[75]: Cmd_: failover link fover GigabitEthernet0/8
[76]: Cmd_: failover interface ip fover 10.0.0.63 255.255.255.0 standby 10.0.0.64
[77]: Cmd_: no failover wait-disable
[78]: Cmd_: no monitor-interface service-module
[79]: Cmd_: icmp unreachable rate-limit 1 burst-size 1
[80]: Cmd_: no asdm history enable
[81]: Cmd_: arp timeout 14400
[82]: Cmd_: no arp permit-nonconnected
[83]: Cmd_: arp rate-limit 32768
[84]: Cmd_: route management 0.0.0.0 0.0.0.0 192.168.2.1 1
[85]: Cmd_: timeout xlate 3:00:00
[86]: Cmd_: timeout pat-xlate 0:00:30
[87]: Cmd_: timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
[88]: Cmd_: timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
[89]: Cmd_: timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
[90]: Cmd_: timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
[91]: Cmd_: timeout tcp-proxy-reassembly 0:01:00
[92]: Cmd_: timeout floating-conn 0:00:00
[93]: Cmd_: timeout conn-holddown 0:00:15
[94]: Cmd_: timeout igp stale-route 0:01:10
[95]: Cmd_: user-identity default-domain LOCAL
[96]: Cmd_: aaa authentication ssh console LOCAL
[97]: Cmd_: aaa authentication login-history
[98]: Cmd_: http server enable
[99]: Cmd_: http 0.0.0.0 0.0.0.0 management
[100]: Cmd_: no snmp-server location
[101]: Cmd_: no snmp-server contact
[102]: Cmd_: crypto ipsec security-association pmtu-aging infinite
[103]: Cmd_: crypto ca trustpoint _SmartCallHome_ServerCA
[104]: Cmd_:  no validation-usage
[105]: Cmd_:  crl configure
[106]: Cmd_: crypto ca trustpoint _SmartCallHome_ServerCA2
[107]: Cmd_:  no validation-usage
[108]: Cmd_:  crl configure
[109]: Cmd_: crypto ca trustpool policy
[110]: Cmd_:  auto-import
[111]: Cmd_: crypto ca certificate chain _SmartCallHome_ServerCA
[112]: Cmd_:  certificate ca 0a0142800000014523c844b500000002
[113]: Cmd_:     30820560 30820348 a0030201 0202100a 01428000 00014523 c844b500 00000230
[114]: Cmd_:     0d06092a 864886f7 0d01010b 0500304a 310b3009 06035504 06130255 53311230
[115]: Cmd_:     10060355 040a1309 4964656e 54727573 74312730 25060355 0403131e 4964656e
[116]: Cmd_:     54727573 7420436f 6d6d6572 6369616c 20526f6f 74204341 2031301e 170d3134
[117]: Cmd_:     30313136 31383132 32335a17 0d333430 31313631 38313232 335a304a 310b3009
[118]: Cmd_:     06035504 06130255 53311230 10060355 040a1309 4964656e 54727573 74312730
[119]: Cmd_:     25060355 0403131e 4964656e 54727573 7420436f 6d6d6572 6369616c 20526f6f
[120]: Cmd_:     74204341 20313082 0222300d 06092a86 4886f70d 01010105 00038202 0f003082
[121]: Cmd_:     020a0282 020100a7 5019de3f 993dd433 46f16f51 6182b2a9 4f8f6789 5d84d953
[122]: Cmd_:     dd0c28d9 d7f0ffae 95437299 f9b55d7c 8ac142e1 315074d1 810d7ccd 9b21ab43
[123]: Cmd_:     e2acad5e 866ef309 8a1f5a32 bda2eb94 f9e85c0a ecff98d2 af71b3b4 539f4e87
[124]: Cmd_:     ef92bcbd ec4f3230 884b175e 57c453c2 f602978d d9622bbf 241f628d dfc3b829
```

```
[125]: Cmd_:     4b49783c 93608822 fc99da36 c8c2a2d4 2c540067 356e73bf 0258f0a4 dde5b0a2
[126]: Cmd_:     267acae0 36a51916 f5fdb7ef ae3f40f5 6d5a04fd ce34ca24 dc74231b 5d331312
[127]: Cmd_:     5dc40125 f630dd02 5d9fe0d5 47bdb4eb 1ba1bb49 49d89f5b 02f38ae4 2490e462
[128]: Cmd_:     4f4fc1af 8b0e7417 a8d17288 6a7a0149 ccb44679 c617b1da 981e0759 fa752185
[129]: Cmd_:     65dd9056 cefbaba5 609dc49d f952b08b bd87f98f 2b230a23 763bf733 e1c900f3
[130]: Cmd_:     69f94ba2 e04ebc7e 93398407 f744707e fe075ae5 b1acd118 ccf235e5 494908ca
[131]: Cmd_:     56c93dfb 0f187d8b 3bc113c2 4d8fc94f 0e37e91f a10e6adf 622ecb35 0651792c
[132]: Cmd_:     c82538f4 fa4ba789 5c9cd2e3 0d39864a 747cd559 87c23f4e 0c5c52f4 3df75282
[133]: Cmd_:     f1eaa3ac fd49341a 28f34188 3a13eee8 deff991d 5fbacbe8 1ef2b950 60c031d3
[134]: Cmd_:     73e5efbe a0ed330b 74be2020 c4676cf0 08037a55 807f464e 96a7f41e 3ee1f6d8
[135]: Cmd_:     09e13364 2b63d732 5e9ff9c0 7b0f786f 97bc939a f99c1290 787a8087 15d77274
[136]: Cmd_:     9c557478 b1bae16e 7004ba4f a0ba68c3 7bff31f0 733d3d94 2ab10b41 0ea0fe4d
[137]: Cmd_:     88656b79 33b4d702 03010001 a3423040 300e0603 551d0f01 01ff0404 03020106
[138]: Cmd_:     300f0603 551d1301 01ff0405 30030101 ff301d06 03551d0e 04160414 ed4419c0
[139]: Cmd_:     d3f0068b eea47bbe 42e72654 c88e3676 300d0609 2a864886 f70d0101 0b050003
[140]: Cmd_:     82020100 0dae9032 f6a64b7c 44761961 1e2728cd 5e54ef25 bce30890 f929d7ae
[141]: Cmd_:     6808e194 0058ef2e 2e7e5352 8cb65c07 ea88ba99 8b5094d7 8280df61 090093ad
[142]: Cmd_:     0d14e6ce c1f23794 78b05f9c b3a273b8 8f059338 cd8d3eb0 b8fbc0cf b1f2ec2d
[143]: Cmd_:     2d1bccec aa9ab3aa 60821b2d 3bc3843d 578a961e 9c75b8d3 30cd6008 8390d38e
[144]: Cmd_:     54f14d66 c05d7403 40a3ee85 7ec21f77 9c06e8c1 a7185d52 95edc9dd 259e6dfa
[145]: Cmd_:     a9eda33a 34d0597b daed50f3 35bfedeb 144d31c7 60f4daf1 879ce248 e2c6c537
[146]: Cmd_:     fb0610fa 75596631 4729da76 9a1ce982 aeef9ab9 51f78823 9a699562 3ce55580
[147]: Cmd_:     36d75402 fff1b95d ced4236f d845844a 5b65ef89 0cdd14a7 20cb18a5 25b40df9
[148]: Cmd_:     01f0a2d2 f400c874 8ea12a48 8e65db13 c4e22517 7debbe87 5b172054 51934a53
[149]: Cmd_:     030bec5d ca33ed62 fd45c72f 5bdc58a0 8039e6fa d7fe1314 a6ed3d94 4a4274d4
[150]: Cmd_:     c3775973 cd8f46be 5538effa e89132ea 97580422 de38c3cc bc6dc933 3a6a0a69
[151]: Cmd_:     3fa0c8ea 728f8c63 8623bd6d 3c969e95 e0494caa a2b92a1b 9c368178 edc3e846
[152]: Cmd_:     e2265944 751ed975 8951cd10 849d6160 cb5df997 224d8e98 e6e37ff6 5bbbaecd
[153]: Cmd_:     ca4a816b 5e0bf351 e1742be9 7e27a7d9 99494ef8 a580db25 0f1c6362 8ac93367
[154]: Cmd_:     6b3c1083 c6addea8 cd168e8d f0073771 9ff2abfc 41f5c18b ec00375d 09e54e80
[155]: Cmd_:     effab15c 3806a51b 4ae1dc38 2d3cdcab 1f901ad5 4a9ceed1 706cccee f457f818
[156]: Cmd_:     ba846e87
[157]: Cmd_:   quit
[158]: Cmd_: crypto ca certificate chain _SmartCallHome_ServerCA2
[159]: Cmd_:  certificate ca 0509
[160]: Cmd_:     308205b7 3082039f a0030201 02020205 09300d06 092a8648 86f70d01 01050500
[161]: Cmd_:     3045310b 30090603 55040613 02424d31 19301706 0355040a 13105175 6f566164
[162]: Cmd_:     6973204c 696d6974 6564311b 30190603 55040313 1251756f 56616469 7320526f
[163]: Cmd_:     6f742043 41203230 1e170d30 36313132 34313832 3730305a 170d3331 31313234
[164]: Cmd_:     31383233 33335a30 45310b30 09060355 04061302 424d3119 30170603 55040a13
[165]: Cmd_:     1051756f 56616469 73204c69 6d697465 64311b30 19060355 04031312 51756f56
[166]: Cmd_:     61646973 20526f6f 74204341 20323082 0222300d 06092a86 4886f70d 01010105
[167]: Cmd_:     00038202 0f003082 020a0282 0201009a 18ca4b94 0d002daf 03298af0 0f81c8ae
[168]: Cmd_:     4c19851d 089fab29 4485f32f 81ad321e 9046bfa3 86261a1e fe7e1c18 3a5c9c60
[169]: Cmd_:     172a3a74 8333307d 615411cb edabe0e6 d2a27ef5 6b6f18b7 0a0b2dfd e93eef0a
[170]: Cmd_:     c6b310e9 dcc24617 f85dfda4 daff9e49 5a9ce633 e62496f7 3fba5b2b 1c7a35c2
[171]: Cmd_:     d667feab 66508b6d 28602bef d760c3c7 93bc8d36 91f37ff8 db1113c4 9c7776c1
[172]: Cmd_:     aeb7026a 817aa945 83e205e6 b956c194 378f4871 6322ec17 6507958a 4bdf8fc6
[173]: Cmd_:     5a0ae5b0 e35f5e6b 11ab0cf9 85eb44e9 f80473f2 e9fe5c98 8cf573af 6bb47ecd
[174]: Cmd_:     d45c022b 4c39e1b2 95952d42 87d7d5b3 9043b76c 13f1dedd f6c4f889 3fd175f5
[175]: Cmd_:     92c391d5 8a88d090 ecdc6dde 89c26571 968b0d03 fd9cbf5b 16ac92db eafe797c
[176]: Cmd_:     adebaff7 16cbdbcd 252be51f fb9a9fe2 51cc3a53 0c48e60e bdc9b476 0652e611
[177]: Cmd_:     13857263 0304e004 362b2019 02e874a7 1fb6c956 66f07525 dc67c10e 616088b3
[178]: Cmd_:     3ed1a8fc a3da1db0 d1b12354 df44766d ed41d8c1 b222b653 1cdf351d dca1772a
[179]: Cmd_:     31e42df5 e5e5dbc8 e0ffe580 d70b63a0 ff33a10f ba2c1515 ea97b3d2 a2b5bef2
[180]: Cmd_:     8c961e1a 8f1d6ca4 6137b986 7333d797 969e237d 82a44c81 e2a1d1ba 675f9507
[181]: Cmd_:     a32711ee 16107bbc 454a4cb2 04d2abef d5fd0c51 ce506a08 31f991da 0c8f645c
[182]: Cmd_:     03c33a8b 203f6e8d 673d3ad6 fe7d5b88 c95efbcc 61dc8b33 77d34432 35096204
[183]: Cmd_:     921610d8 9e2747fb 3b21e3f8 eb1d5b02 03010001 a381b030 81ad300f 0603551d
[184]: Cmd_:     130101ff 04053003 0101ff30 0b060355 1d0f0404 03020106 301d0603 551d0e04
[185]: Cmd_:     1604141a 8462bc48 4c332504 d4eed0f6 03c41946 d1946b30 6e060355 1d230467
[186]: Cmd_:     30658014 1a8462bc 484c3325 04d4eed0 f603c419 46d1946b a149a447 3045310b
[187]: Cmd_:     30090603 55040613 02424d31 19301706 0355040a 13105175 6f566164 6973204c
[188]: Cmd_:     696d6974 6564311b 30190603 55040313 1251756f 56616469 7320526f 6f742043
```

```
[189]: Cmd_:     41203282 02050930 0d06092a 864886f7 0d010105 05000382 0201003e 0a164d9f
[190]: Cmd_:     065ba8ae 715d2f05 2f67e613 4583c436 f6f3c026 0c0db547 645df8b4 72c946a5
[191]: Cmd_:     03182755 89787d76 ea963480 1720dce7 83f88dfc 07b8da5f 4d2e67b2 84fdd944
[192]: Cmd_:     fc775081 e67cb4c9 0d0b7253 f8760707 4147960c fbe08226 93558cfe 221f6065
[193]: Cmd_:     7c5fe726 b3f73290 9850d437 7155f692 2178f795 79faf82d 26876656 3077a637
[194]: Cmd_:     78335210 58ae3f61 8ef26ab1 ef187e4a 5963ca8d a256d5a7 2fbc561f cf39c1e2
[195]: Cmd_:     fb0aa815 2c7d4d7a 63c66c97 443cd26f c34a170a f890d257 a21951a5 2d9741da
[196]: Cmd_:     074fa950 da908d94 46e13ef0 94fd1000 38f53be8 40e1b46e 561a20cc 6f588ded
[197]: Cmd_:     2e458fd6 e9933fe7 b12cdf3a d6228cdc 84bb226f d0f8e4c6 39e90488 3cc3baeb
[198]: Cmd_:     557a6d80 9924f56c 01fbf897 b0945beb fdd26ff1 77680d35 6423acb8 55a103d1
[199]: Cmd_:     4d4219dc f8755956 a3f9a849 79f8af0e b911a07c b76aed34 d0b62662 381a870c
[200]: Cmd_:     f8e8fd2e d3907f07 912a1dd6 7e5c8583 99b03808 3fe95ef9 3507e4c9 626e577f
[201]: Cmd_:     a75095f7 bac89be6 8ea201c5 d666bf79 61f33c1c e1b9825c 5da0c3e9 d848bd19
[202]: Cmd_:     a2111419 6eb2861b 683e4837 1a88b75d 965e9cc7 ef276208 e291195c d2f121dd
[203]: Cmd_:     ba174282 97718153 31a99ff6 7d62bf72 e1a3931d cc8a265a 0938d0ce d70d8016
[204]: Cmd_:     b478a53a 874c8d8a a5d54697 f22c10b9 bc5422c0 01506943 9ef4b2ef 6df8ecda
[205]: Cmd_:     f1e3b1ef df918f54 2a0b25c1 2619c452 100565d5 8210eac2 31cd2e
[206]: Cmd_:   quit
[207]: Cmd_: telnet timeout 5
[208]: Cmd_: ssh stack ciscossh
[209]: Cmd_: ssh stricthostkeycheck
[210]: Cmd_: ssh timeout 5
[211]: Cmd_: ssh key-exchange group dh-group14-sha256
[212]: Cmd_: ssh 0.0.0.0 0.0.0.0 management
[213]: Cmd_: console timeout 0
[214]: Cmd_: console serial
[215]: Cmd_: threat-detection basic-threat
[216]: Cmd_: threat-detection statistics access-list
[217]: Cmd_: no threat-detection statistics tcp-intercept
[218]: Cmd_: dynamic-access-policy-record DfltAccessPolicy
[219]: Cmd_: username admin password
$sha512$5000$w9Jv9lDWNVn4XKSG1i0G6Q==$JgmsMmRSYz+ZQX3Ta/bXxA== pbkdf2 privilege 15
[220]: Cmd_: !
[221]: Cmd_: class-map inspection_default
[222]: Cmd_:  match default-inspection-traffic
[223]: Cmd_: !
[224]: Cmd_: !
[225]: Cmd_: policy-map type inspect dns preset_dns_map
[226]: Cmd_:  parameters
[227]: Cmd_:   message-length maximum client auto
[228]: Cmd_:   message-length maximum 512
[229]: Cmd_:   no tcp-inspection
[230]: Cmd_: policy-map global_policy
[231]: Cmd_:  class inspection_default
[232]: Cmd_:   inspect ip-options
[233]: Cmd_:   inspect netbios
[234]: Cmd_:   inspect rtsp
[235]: Cmd_:   inspect sunrpc
[236]: Cmd_:   inspect tftp
[237]: Cmd_:   inspect dns preset_dns_map
[238]: Cmd_:   inspect ftp
[239]: Cmd_:   inspect h323 h225
[240]: Cmd_:   inspect h323 ras
[241]: Cmd_:   inspect rsh
[242]: Cmd_:   inspect esmtp
[243]: Cmd_:   inspect sqlnet
[244]: Cmd_:   inspect sip
[245]: Cmd_:   inspect skinny
[246]: Cmd_: policy-map type inspect dns migrated_dns_map_2
[247]: Cmd_:  parameters
[248]: Cmd_:   message-length maximum client auto
[249]: Cmd_:   message-length maximum 512
[250]: Cmd_:   no tcp-inspection
[251]: Cmd_: policy-map type inspect dns migrated_dns_map_1
```

```
[252]: Cmd_:  parameters
[253]: Cmd_:   message-length maximum client auto
[254]: Cmd_:   message-length maximum 512
[255]: Cmd_:   no tcp-inspection
[256]: Cmd_: !
[257]: Cmd_: service-policy global_policy global
[258]: Cmd_: prompt hostname context
[259]: Cmd_: call-home reporting anonymous prompt 1
[260]: Cmd_: call-home
[261]: Cmd_:  profile License
[262]: Cmd_:   destination address http
https://sch-alpha.cisco.com/its/service/oddce/services/DDCEService
[263]: Cmd_:   destination transport-method http
[264]: Cmd_:  profile CiscoTAC-1
[265]: Cmd_:   no active
[266]: Cmd_:   destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
[267]: Cmd_:   destination address email callhome@cisco.com
[268]: Cmd_:   destination transport-method http
[269]: Cmd_:   subscribe-to-alert-group diagnostic
[270]: Cmd_:   subscribe-to-alert-group environment
[271]: Cmd_:   subscribe-to-alert-group inventory periodic monthly
[272]: Cmd_:   subscribe-to-alert-group configuration periodic monthly
[273]: Cmd_:   subscribe-to-alert-group telemetry periodic daily
My State: Negotiation
Config content_size: 11323
Config Hash: 9d653d6fb48739651f5467a1aebea31c
```

The following are the sample output from the **showfailoverconfig-syncstatus** command when Config Sync Optimization feature is enabled on the device.

```
ciscoasa# show failover config-sync status
Config Sync Optimization is enable
```

Related Commands

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

show fault-monitor block-depletion

To view the status and statistical details on the block depletion, use the **show fault-monitor block-depletion** command.

show fault-monitor block-depletion { **status** | **statistics** }

Syntax Description

status	Displays status on the block depletion.
statistics	Displays statistical details on the block depletion.

Command Default

No default behavior or values.

Command History

Release	Modification
9.22(3)	This command was added.

Usage Guidelines

This command displays the status and statistical details on the block depletion.

Examples

The following is sample output for the **show fault-monitor block-depletion status** :

```
ciscoasa# show fault-monitor block-depletion status
Block-Depletion: [ENABLED]
Block-Depletion Current State [2]: Monitoring State
Recovery action configured = [Reload]
Block-Depletion - monitor-interval [60] sec
```

The following is sample output for the **show fault-monitor block-depletion statistics** command:

```
ciscoasa# show fault-monitor block-depletion statistics

Current time 146434260 msec

                        Block depletion statistics

 blk sz          CF         MET         DST        < 1s       < 10s        >10s     Max(sec)
-------          --         ---         ---        ----       -----        ----     -------

      0           0           0           0           0           0           0
0

      4           0           0           0           0           0           0
0

     80           0           0           0           0           0           0
0

    256           0           0           0           0           0           0
0

   1550           0           0           0           0           0           0
0

   2048           0           0           0           0           0           0
```

```
0

   2560           0           0           0           0           0           0
0

   4096           0           0           0           0           0           0
0

   8192           0           0           0           0           0           0
0

   9344           0           0           0           0           0           0
0

  16384           0           0           0           0           0           0
0

  65664           0           0           0           0           0           0
0

   2048           0           0           0           0           0           0
0
```

```
CF = Number of consecutive alloc failures without an intervening alloc success
MET = Fault monitor end timestamp before recovery action is triggered
DST = Timestamp of when most recent block depletion started
< 1s = Number of times block depleted duration was less than 1s
< 10s = Number of times block depleted duration was less than 10s but greater than 1s
> 10s = Number of times block depleted duration was greater than 10s
Max = Max block-depleted-duration so far in seconds
ciscoasa/act#
```

show fault-monitor mbuf-depletion

To view the status and statistical details on the MBUF depletion, use the **show fault-monitor mbuf-depletion** command.

show fault-monitor mbuf-depletion status

Syntax Description

status	Displays status on the MBUF pool depletion.

Command Default

No default behavior or values.

Command History

Release	Modification
9.24(10)	This command was added.

Usage Guidelines

This command displays the status on the mbuf pool depletion.

Examples

The following is sample output for the **show fault-monitor mbuf-depletion status** :

```
ciscoasa# show fault-monitor mbuf-depletion status
MBUF-Depletion: [ENABLED]
MBUF-Depletion Current State [2]: Monitoring State
Recovery action configured = [Reload]
MBUF-Depletion - monitor-interval [60] sec
```

show file

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

show file descriptors | system | information *filename*

Syntax Description

descriptors	Displays all open file descriptors.
filename	Specifies the filename.
information	Displays information about a specific 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 Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	The capability to view information about partner application package files was added.
9.7(1)	The **show file descriptor** command was updated to print the output, only from the open file descriptor in the system context mode.

Usage Guidelines

The **show file descriptors** command when used in System context in Multi context mode, it traverses through all the contexts and displays details of file descriptors if they are opened. If a context has an open file descriptor, only the details of that specific context is displayed, when the CLI is executed in the System context. The system does not print all the names of the context with “no file descriptors”. Only the context with open file descriptor is displayed.

Examples

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

Single context with no open file

```
ciscoasa(config)# show file descriptors
```

```
No open file descriptors
ciscoasa(config)#
```

Single context with open files

```
ciscoasa(config)# show file descriptors
FD  Position  Open  PID  Path
0 0 0302  139  disk0:/test1.txt
ciscoasa(config)#
```

Multicontext with no open files in the System context

```
ciscoasa# show file descriptors
ciscoasa#
```

Multicontext with open files in the System context

```
ST-Campus-spyc/stby(config)# show file descriptors
Context: CTX1
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
Context: CTX3
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
Context: CTX5
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
```

Multicontext with no open files in the User context

```
ST-Campus-spyc/stby/CTX1(config)# changeto context CTX2
ST-Campus-spyc/act/CTX2(config)# show file descriptors
No open file descriptors
ST-Campus-spyc/act/CTX2(config)#
```

Multicontext with open files in the User context

```
ST-Campus-spyc/stby(config)# changeto con CTX1
ST-Campus-spyc/stby/CTX1(config)# show file descriptors
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
ST-Campus-spyc/stby/CTX1(config)#
ciscoasa# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

The following is sample output from the **show file info** command:

```
ciscoasa# show file info disk0:csc_embd1.0.1000.pkg
type is package (csc)
file size is 17204149 bytes version 1
```

Related Commands

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

show fips

To show the FIPS status, use the **show fips** command in privileged EXEC mode.

show fips

Command Modes

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

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

Command History

Release	Modification
9.13(1)	This command was added.

Usage Guidelines

The **show running-configuration fips** command displays whether FIPS is enabled. The **show fips** command displays the current operational state of FIPS. This command also displays status for rebooting the device after an enable or disable action.

Examples

When FIPS is disabled and a user enables it by running **fips enable**

```
ciscoasa# show fips
FIPS is currently disabled and will be enabled after reboot
```

After the device is rebooted,

```
ciscoasa# show fips
FIPS is currently enabled
```

When FIPS is enabled and a user disables it by running **no fips enable**:

```
ciscoasa# show fips
FIPS is currently enabled and will be disabled after reboot
```

After the device is rebooted,

```
ciscoasa# show fips
FIPS is currently disabled
```

Related Commands

Command	Description
fips enable	Enables FIPS on ASA.

Command	Description
show running-configuration fips	Shows the current running and operational configuration of fips.

show firewall

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

show firewall

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

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

Related Commands

Command	Description
firewall transparent	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 in privileged EXEC mode.

show flash: all | controller | filesys

Note In the ASA, 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 Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

```
ciscoasa# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
```

```
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 06:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log
10170368 bytes available (52711424 bytes used)
```

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 display runtime counters associated with NetFlow data, use the **show flow-export counters** command in privileged EXEC mode.

show flow-export counters

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.1(1)	This command was added.
9.0(1)	A new error counter was added for source port allocation failure.

Usage Guidelines

The runtime counters include statistical data as well as error data.

Examples

The following is sample output from the **show flow-export counters** command, which shows runtime counters that are associated with NetFlow data:

```
ciscoasa# 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

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

Commands	Description
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.

show flow-offload

To display information about flow off-loading, use the **show flow-offload** command in privileged EXEC mode.

show flow-offload { **info** [**detail**] | **cpu** | **flow** [**count** | **detail** | **protocol** *type*] | **statistics** }

Syntax Description

info [**detail**]	Shows basic information about the offload engine. Add the **detail** keyword to get additional information such as a summary of port usage.
cpu	Shows the load percentage on offload cores.
flow [**count** | **detail** | **protocol** *type*]	Shows information on the active off-loaded flows. You can optionally add the following keywords: • **count** —Shows the number of off-loaded active flows and offloaded flows created. • **detail** —Shows the active off-loaded flows and their rewrite rules and data. • **protocol** *type* —Shows flows by protocol.
statistics	Shows the packet statistics of off-loaded flows.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.23(1)	For the **flow** option, added statistics for cluster redirect flows. Also added the flow protocol option for For the **info** option, added output about whether cluster redirect is enabled.
9.22(1)	Added destination IP and port to output for GRE traffic. Added support for the Secure Firewall 3100.
9.5(2)	This command was introduced.

Usage Guidelines

If you enable flow off-loading, use this command to view information about the service and the off-loaded flows.

Examples

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.

For GRE traffic, source IP, Source Port, Destination IP and Destination Port are shown in the output.

```
>show flow-offload flow
Total offloaded flow stats: 1 in use, 5 most used, 100% offloaded, 0 collisions
UDP intfc 103 src 10.1.1.2:41110 dest 20.1.1.2:5001, dynamic, timestamp 162810457, packets
 84040, bytes 127404640
GRE intfc 102 src 20.20.20.20:0 dest 5.5.5.5:0, timestamp 4208449953972, packets 5, bytes
550
GRE intfc 101 src 5.5.5.5:0 dest 20.20.20.20:0, timestamp 4209570830802, packets 6, bytes
674
```

The following is sample output from the **show flow-offload statistics** command. The output shows counts for transmitted (Tx), received (Rx) and dropped packets, and statistics for the virtual NIC (VNIC) used.

```
ciscoasa# show offload-engine statistics

Packet stats of port : 0
        Tx Packet count                 :        785807566
        Rx Packet count                 :        785807566
        Dropped Packet count            :                0
        VNIC transmitted packet         :        785807566
        VNIC transmitted bytes          :     103726598712
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
 Packet stats of port : 1
        Tx Packet count                 :                0
        Rx Packet count                 :                0
        Dropped Packet count            :                0
        VNIC transmitted packet         :                0
        VNIC transmitted bytes          :                0
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
```

Following is an example of information detail.

```
ciscoasa(config)# show flow-offload info detail

Current running state        : Enabled
User configured state        : Enabled
Dynamic flow offload         : Enabled
Offload App                  : Running
Offload allocated cores      : S0[ 2]
Offload Nic                  : 9
Max PKT burst                : 32
```

```
Port-0 details :
        FQ queue number      :           1440
        Keep alive counter   :         101584
flow table refresh count     : 186 [58]
HW flow table refresh count  : Port-0[58, 58, 58, 58]
Refresh count synched        : 3 times [3/0]
Flow table status Port-0     : Good
GRE intfc 102 src 20.20.20.20:0 dest 5.5.5.5:0, timestamp 4208449953972, packets 5, bytes
550
GRE intfc 101 src 5.5.5.5:0 dest 20.20.20.20:0, timestamp 4209570830802, packets 6, bytes
674
```

For GRE traffic, source IP, Source Port, Destination IP and Destination Port are shown in the output.

The refresh count information at the bottom of the output indicates the status of the flow tables kept in software (ASA) and hardware. The “refresh count” is the number of times the flow-table was invalidated, which could be due to multiple events such as route changes (addition/deletion) from software to hardware, MAC address change, and so forth.

- Flow table refresh count is the number of times the flow-table needed be invalidated. This value is maintained in ASA software.
- HW flow table refresh count is the number of times the hardware flow-table was invalidated. This value is maintained in the hardware.
- Refresh count synched is the number of times the “flow table refresh count” is explicitly synchronized from software to hardware. This happens whenever there was a mismatch between them. Normally, “flow table refresh count” and “HW flow table refresh count” will be in sync and there is no need to synchronize those values explicitly. Normally, the parameter “Refresh count synched” will be zero.
- “Flow table status” is either Good or Bad. Good indicates that “flow table refresh count” and “HW flow table refresh count” are in sync. Bad indicates a mismatch, even after trying to explicitly synchronize them. This could happen in rare condition like the CRUZ firmware is stuck or unresponsive for any update requests from the ASA software.

The following example of **show flow-offload flow** shows the statistics of the offloaded cluster-redirect connections. This output shows the percentage of the total number of flows. So, if there are more than 400 flows and only two are offloaded, the percentage will show as zero (0.5% is rounded off to zero).

```
WA-45(config)# show flow-offload flow
2 in use, 3 most used, 0% offloaded, 0 collisions
TCP intfc 1001 src 14.14.14.243:9998 dest 11.11.11.243:39524, timestamp 9747249142136,
packets 88019121, bytes 7569644406
TCP intfc 1001 src 14.14.14.243:9998 dest 11.11.11.243:39534, timestamp 9747809181462,
packets 88526595, bytes 7613287198
```

The **show flow-offload flow protocol esp** command shows flows using the ESP protocol:

```
RTP-Cluster# show flow-offload flow protocol esp
ESP intfc 0 src 10.10.0.12:60729 dest 10.10.0.1:35232, timestamp 3542470428259, packets
277, bytes 300406
```

Related Commands

Command	Description
clear flow-offload	Clears off-load statistics or flows.

Command	Description
flow-offload	Enables flow off-load.
set-connection advanced-options flow-offload	Identifies traffic flows as eligible for off-load.

show flow-offload-ipsec

To display information about IP sec flow off-loading, use the **show flow-offload-ipsec** command in privileged EXEC mode.

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 Default

No defaults.

Command Modes

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

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

Command History

Release	Modification
9.18(1)	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.

```
ciscoasa# 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.

```
ciscoasa# 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.
flow-offload-ipsec	Configures IPsec flow offload.

show fragment

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

show fragment [*interface*]

Syntax Description

interface	(Optional) Specifies the ASA interface.

Command Default

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The command was separated into two commands, **show fragment** and **show running-config fragment**, to separate the configuration data from the operational data.
9.15(1)	The output for the **show fragment** command was enhanced to include IP fragment related drops and error counters.

Examples

This example displays the operational data of the IP fragment reassembly module:

```
ciscoasa# 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.
- Runtime stats: Queue. The number of fragments in the reassembly database currently awaiting reassembly.
- Runtime stats: Full Assembly. The number of IP packets fully reassembled.
- 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.
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show running-config fragment	Displays the IP fragment reassembly configuration.

show fxos mode

To view the Firepower 2100 mode, Appliance or Platform, use the **show fxos mode** command in privileged EXEC mode.

show fxos mode

Note This command is supported on the Firepower 2100 only.

Syntax Description

This command has no arguments or keywords.

Command Default

The mode is set to Appliance mode by default.

Command Modes

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

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

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

The Firepower 2100 runs an underlying operating system called FXOS. You can run the Firepower 2100 in the following modes:

- Appliance mode (the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI.
- Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the Secure Firewall Chassis Manager (formerly Firepower Chassis Manager) web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI.

Use the **show fxos mode** to view the current mode.

Examples

The following is sample output from the **show fxos mode** command:

```
ciscoasa# show fxos mode
Mode is currently set to appliance
```

Related Commands

Command	Description
connect fxos	Connects to the FXOS CLI.
fxos mode appliance	Sets the mode to Appliance mode.

show gc

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

show gc

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

```
ciscoasa# 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 ASA, use the show **h225** command in privileged EXEC mode.

show h225

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show h225** command displays information for H.225 sessions established across the ASA.

Before using the **show h225**, **show h245**, or **show h323 ras** commands, we recommend that you configure the **pager** command. If there are a lot of session records and the **pager** command is not configured, it may take a while for the **show** output to reach its end.

If there is an abnormally large number of connections, check that the sessions are timing out based on the default timeout values or the values set by you. If they are not, then there is a problem that needs to be investigated.

Examples

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

```
ciscoasa# 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 ASA 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
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the ASA by endpoints using slow start.
show h323 ras	Displays information for H.323 RAS sessions established across the ASA.
timeout h225 | **h323**	Configures idle time after which an H.225 signaling connection or an H.323 control connection will be closed.

show h245

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

show h245

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show h245** command displays information for H.245 sessions established across the ASA 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:

```
ciscoasa# 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 ASA. 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
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the ASA by endpoints using slow start.
show h323 ras	Displays information for H.323 RAS sessions established across the ASA.
timeout h225 | **h323**	Configures idle time after which an H.225 signaling connection or an H.323 control connection will be closed.

show h323

To display information for H.323 connections, use the show **h323** command in privileged EXEC mode.

show h323 { **ras | gup** }

Syntax Description

ras	Displays the H323 RAS sessions established across the ASA between a gatekeeper and its H.323 endpoint.
gup	Displays information about the H323 gateway updated protocol connections.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show h323 ras** command displays information for H.323 RAS sessions established across the ASA between a gatekeeper and its H.323 endpoint.

Examples

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

```
ciscoasa# show h323 ras
ciscoasa#
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
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the ASA by endpoints using slow start.

Commands	Description
timeout h225 | **h323**	Configures idle time after which an H.225 signaling connection or an H.323 control connection will be closed.

show hardware-bypass

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

show hardware-bypass

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.4(1.225)	This command was added.

Examples

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

```
ciscoasa# 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
```

Related Commands

Commands	Description
hardware-bypass	Configures hardware bypass mode on an ISA 3000 device.

show history

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

show history

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

Examples

The following example shows sample output from the **show history** command in user EXEC mode:

```
ciscoasa> show history
show history
help
show history
```

The following example shows sample output from the **show history** command in privileged EXEC mode:

```
ciscoasa
#
 show history
show history
help
show history
enable
show history
```

The following example shows sample output from the **show history** command in global configuration mode:

```
ciscoasa(config)#
show history
show history
help
show history
enable
show history
config t
show history
```

Related Commands

Command	Description
help	Displays help information for the command specified.

show hostname

To show the hostname, use the **show hostname** command in privileged EXEC mode.

show hostname [**fqdn**]

Syntax Description

fqdn	Shows the fully-qualified domain name.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Command added.

Usage Guidelines

Set the hostname using the **hostname** command, and set the domain using the **domain-name** command.

Examples

The following is sample output from the show hostname fqdn command:

```
ciscoasa# show hostname fqdn
asa1.cisco.com
```

Related Commands

Command	Description
hostname	Sets the ASA hostname.
domain-name	Sets the domain name for the ASA.

show icmp

To display the ICMP configuration, use the show icmp command in privileged EXEC mode.

show icmp

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command already existed.

Usage Guidelines

The **show icmp** command displays the ICMP configuration.

Examples

The following example shows the ICMP configuration:

```
ciscoasa# show icmp
```

Related Commands

clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debugging information for ICMP.
icmp	Configures access rules for ICMP traffic that terminates at an ASA interface.
inspect icmp	Enables or disables the ICMP inspection engine.
timeout icmp	Configures the idle timeout for ICMP.

show idb

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

show idb

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

Examples

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

```
ciscoasa# show idb
Maximum number of Software IDBs 280. In use 23.
                   HWIDBs     SWIDBs
            Active 6          21
          Inactive 1          2
         Total IDBs 7          23
 Size each (bytes) 116        212
       Total bytes 812        4876
HWIDB#  1 0xbb68ebc  Control0/0
HWIDB#  2 0xcd47d84  GigabitEthernet0/0
HWIDB#  3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#  4 0xcd5063c  GigabitEthernet0/2
HWIDB#  5 0xcd54a9c  GigabitEthernet0/3
HWIDB#  6 0xcd58f04  Management0/0
SWIDB#  1 0x0bb68f54 0x01010001 Control0/0
SWIDB#  2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#  3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
```

```
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

Table 7-4 shows each field description.

Table 4: show idb stats Fields

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

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show igmp groups

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

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

Examples

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

```
ciscoasa# show igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

Related Commands

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

show igmp interface

To display multicast information for an interface, use the **show igmp interface** command in privileged EXEC mode.

show igmp interface [*if_name*]

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was modified. The **detail** keyword was removed.

Usage Guidelines

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

Examples

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

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

Related Commands

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

show igmp traffic

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

show igmp traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

```
ciscoasa# show igmp traffic
IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                              Received     Sent
Valid IGMP Packets               3           6
Queries                          2           6
Reports                          1           0
Leaves                           0           0
Mtrace packets                   0           0
DVMRP packets                    0           0
PIM packets                      0           0
Errors:
Malformed Packets                0
Martian source                   0
Bad Checksums                    0
```

Related Commands

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

show import webvpn

To list the files, customization objects, translation tables, or plug-ins in flash memory that customize and localize the ASA or the Secure Client, use the **show import webvpn** command in privileged EXEC mode.

show import webvpn { **AnyConnect-customization | customization | mst-translation | plug-in | translation-table | url-list | webcontent** } [**detailed | xml-output**]

Syntax Description

AnyConnect-customization	Displays resource files, executable files, and MS transforms in the ASA flash memory that customize the Secure Client GUI.
customization	Displays XML customization objects in the ASA flash memory that customize the clientless VPN portal (filenames base64 decoded).
mst-translation	Displays MS transforms in the ASA flash memory that translate the Secure Client installer program.
plug-in	Displays plug-in modules in the ASA flash memory (third-party Java-based client applications, including SSH, VNC, and RDP).
translation-table	Displays translation tables in the ASA flash memory that translate the language of user messages displayed by the clientless portal, Secure Desktop, and plug-ins.
url-list	Displays URL lists in the ASA flash memory used by the clientless portal (filenames base64 decoded).
webcontent	Displays content in ASA flash memory used by the clientless portal, clientless applications, and plugins for online help visible to end users.
detailed	Displays the path in flash memory of the file(s) and the hash.
xml-output	Displays the XML of the file(s).

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Release	Modification
8.2(1)	The AnyConnect-customization keyword was added.

Usage Guidelines

Use the **show import webvpn** command to identify the custom data and the Java-based client applications available to clientless SSL VPN users. The displayed list itemizes all of the requested data types that are in flash memory on the ASA.

Examples

The following illustrates the WebVPN data displayed by various **show import webvpn** command:

```
ciscoasa# show import webvpn plug
ssh
rdp
vnc
ciscoasa#
ciscoasa#  show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tue, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTsPnjdBOo= Tue, 15 Sep 2009 23:23:56 GMT
rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT
ciscoasa# show import webvpn customization

Template
DfltCustomization
ciscoasa#
ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  ru                                                customization
  ua                                                customization
ciscoasa#
ciscoasa# show import webvpn url-list

Template
No bookmarks are currently defined
ciscoasa#
ciscoasa# show import webvpn webcontent
No custom webcontent is loaded
ciscoasa#
```

Related Commands

Command	Description
revert webvpn all	Removes all WebVPN data and plug-in current on the ASA.

show interface

To view interface statistics, use the **show interface** command in privileged EXEC mode.

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

Syntax Description

detail	(Optional) Shows detailed interface information, including the order in which the interface was added, the configured state, the actual state, and asymmetrical routing statistics, if enabled by the **asr-group** command. If you show all interfaces, then information about the internal interfaces for SSMs displays, if installed on the ASA 5500. The internal interface is not user-configurable, and the information is for debugging purposes only.
interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabit** **ethernet 0/1** . See the **interface** command for accepted values.
redundant *number*	(Optional) Identifies the redundant interface ID, such as **redundant** **1** .
stats	(Default) Shows interface information and statistics. This keyword is the default, so this keyword is optional.
summary	(Optional) For a VNI interface, shows only the VNI interface parameters.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For the Firepower 1010, ASA 5505, or ASASM, specifies the VLAN interface.
vni *id*	(Optional) Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.

Command Default

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was modified to include the new interface numbering scheme, and to add the **stats** keyword for clarity, and the **detail** keyword.
7.0(4)	Support for the 4GE SSM interfaces was added.
7.2(1)	Support for switch interfaces was added.
8.0(2)	Support for redundant interfaces was added. Also, the delay is added for subinterfaces. Two new counters were added: input reset drops and output reset drops.
8.2(1)	The no buffer number was changed to show the number of failures from block allocations.
8.6(1)	Support for the ASA 5512-X through ASA 5555-X shared management interface and the control plane interface for the software module were added. The management interface is displayed using the **show interface detail** command as Internal-Data0/1; the control plane interface is displayed as Internal-Control0/0.
9.4(1)	The **vni** interface type was added.
9.5(1)	Clustering site-specific MAC addresses were added to the output.
9.10(1)	For the Firepower 2100/4100/9300, the output of the command is enhanced to indicate the supervisor association status of the interfaces.
9.13(1)	We added support for the Firepower 1000 series and Firepower 2100 in Appliance mode.
9.17(1)	For VNI interfaces, shows if single-arm proxy is enabled. For the Secure Firewall 3100, shows the FEC mode and for the **detail** option, the egress interface for a queue.

Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the ASA shows only statistics for the current context. When you enter this command in the system execution space for a physical interface, the ASA shows the combined statistics for all contexts.

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

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context. If you set the **visible** keyword in the **allocate-interface** command, the ASA shows the interface ID in the output of the **show interface** command.

Note The number of bytes transmitted or received in the Hardware count and the Traffic Statistics count are different.In the hardware count, the amount is retrieved directly from hardware, and reflects the Layer 2 packet size. While in traffic statistics, it reflects the Layer 3 packet size.The count difference is varied based upon the design of the interface card hardware.For example, for a Fast Ethernet card, the Layer 2 count is 14 bytes greater than the traffic count, because it includes the Ethernet header. On the Gigabit Ethernet card, the Layer 2 count is 18 bytes greater than the traffic count, because it includes both the Ethernet header and the CRC.

See the “Examples” section for a description of the display output.

Examples

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

```
ciscoasa# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1328522 packets input, 124426545 bytes, 0 no buffer
        Received 1215464 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124606 packets output, 86803402 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c44f, MTU 1500
        IP address 10.10.0.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c450, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
```

```
       0 packets output, 0 bytes, 0 underruns
       0 output errors, 0 collisions
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops
       input queue (curr/max packets): hardware (0/0)
       output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "faillink":
       0 packets input, 0 bytes
       1 packets output, 28 bytes
       0 packets dropped
     1 minute input rate 0 pkts/sec,  0 bytes/sec
     1 minute output rate 0 pkts/sec,  0 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec,  0 bytes/sec
     5 minute output rate 0 pkts/sec,  0 bytes/sec
     5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
       Auto-Duplex, Auto-Speed
       Active member of Redundant5
       MAC address 000b.fcf8.c451, MTU not set
       IP address unassigned
       0 packets input, 0 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       0 L2 decode drops
       0 packets output, 0 bytes, 0 underruns
       0 output errors, 0 collisions
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops
       input queue (curr/max packets): hardware (0/0)
       output queue (curr/max packets): hardware (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps, DLY 1000 usec
       Auto-Duplex, Auto-Speed
       Available but not configured via nameif
       MAC address 000b.fcf8.c44d, MTU not set
       IP address unassigned
       0 packets input, 0 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       0 L2 decode drops
       0 packets output, 0 bytes, 0 underruns
       0 output errors, 0 collisions, 0 interface resets
       0 babbles, 0 late collisions, 0 deferred
       0 lost carrier, 0 no carrier
       input queue (curr/max packets): hardware (128/128) software (0/0)
       output queue (curr/max packets): hardware (0/0) software (0/0)
Interface Redundant1 "", is down, line protocol is down
  Redundancy Information:
       Members unassigned
Interface Redundant5 "redundant", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
       Auto-Duplex, Auto-Speed
       MAC address 000b.fcf8.c451, MTU 1500
       IP address 10.2.3.5, subnet mask 255.255.255.0
       0 packets input, 0 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       0 L2 decode drops
       0 packets output, 0 bytes, 0 underruns
       0 output errors, 0 collisions
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops
```

```
        input queue (curr/max packets): hardware (0/0) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
  Traffic Statistics for "redundant":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
        Member GigabitEthernet0/3(Active), GigabitEthernet0/2
        Last switchover at 15:15:26 UTC Oct 24 2006
Interface Redundant5.1 "", is down, line protocol is down
        VLAN identifier none
        Available but not configured with VLAN or via nameif
```

The following output shows the use of the site MAC address when in use:

```
ciscoasa# show interface port-channel1.3151
Interface Port-channel1.3151 "inside", is up, line protocol is up
Hardware is EtherChannel/LACP, BW 1000 Mbps, DLY 10 usec
VLAN identifier 3151
MAC address aaaa.1111.1234, MTU 1500
Site Specific MAC address aaaa.1111.aaaa
IP address 10.3.1.1, subnet mask 255.255.255.0
Traffic Statistics for "inside":
132269 packets input, 6483425 bytes
1062 packets output, 110448 bytes
98530 packets dropped
```

Table 7-5 shows each field description.

Table 5: show interface Fields

Field	Description
Interface *ID*	The interface ID. Within a context, the ASA shows the mapped name (if configured), unless you set the **allocate-interface** command **visible** keyword.
"*interface_name* "	The interface name set with the **nameif** command. In the system execution space, this field is blank because you cannot set the name in the system. If you do not configure a name, the following message appears after the Hardware line: `Available but not configured via nameif`
is *state*	The administrative state, as follows: • up—The interface is not shut down. • administratively down—The interface is shut down with the **shutdown** command.

Field	Description
Line protocol is *state*	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.
VLAN identifier	For subinterfaces, the VLAN ID.
Hardware	The interface type, maximum bandwidth, delay, duplex, and speed. When the link is down, the duplex and speed show the configured values. When the link is up, these fields show the configured values with the actual settings in parentheses. The following list describes the common hardware types: • i82542 - Intel PCI Fiber Gigabit card used on PIX platforms • i82543 - Intel PCI-X Fiber Gigabit card used on PIX platforms • i82546GB - Intel PCI-X Copper Gigabit used on ASA platforms • i82547GI - Intel CSA Copper Gigabit used as backplane on ASA platforms • i82557 - Intel PCI Copper Fast Ethernet used on ASA platforms • i82559 - Intel PCI Copper Fast Ethernet used on PIX platforms • VCS7380 - Vitesse Four Port Gigabit Switch used in SSM-4GE
Media-type	(For 4GE SSM interfaces only) Shows if the interface is set as RJ-45 or SFP.

message area	A message might be displayed in some circumstances. See the following examples:
	• In the system execution space, you might see the following message:
	`Available for allocation to a context`
	• If you do not configure a name, you see the following message:
	`Available but not configured via nameif`
	• If an interface is a member of a redundant interface, you see the following message:
	`Active member of Redundant5`

MAC address	The interface MAC address.
Site Specific MAC address	For clustering, shows an in-use site-specific MAC address.
MTU	The maximum size, in bytes, of packets allowed on this interface. If you do not set the interface name, this field shows “MTU not set.”

Field	Description
IP address	The interface IP address set using the **ip address** command or received from a DHCP server. In the system execution space, this field shows "IP address unassigned" because you cannot set the IP address in the system.
Subnet mask	The subnet mask for the IP address.
Packets input	The number of packets received on this interface.
Bytes	The number of bytes received on this interface.
No buffer	The number of failures from block allocations.
Received:	
Broadcasts	The number of broadcasts received.
Input errors	The number of total input errors, including the types listed below. Other input-related errors can also cause the input error count to increase, and some datagrams might have more than one error; therefore, this sum might exceed the number of errors listed for the types below.
Runts	The number of packets that are discarded because they are smaller than the minimum packet size, which is 64 bytes. Runts are usually caused by collisions. They might also be caused by poor wiring and electrical interference.
Giants	The number of packets that are discarded because they exceed the maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
CRC	The number of Cyclical Redundancy Check errors. When a station sends a frame, it appends a CRC to the end of the frame. This CRC is generated from an algorithm based on the data in the frame. If the frame is altered between the source and destination, the ASA notes that the CRC does not match. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Frame	The number of frame errors. Bad frames include packets with an incorrect length or bad frame checksums. This error is usually the result of collisions or a malfunctioning Ethernet device.
Overrun	The number of times that the ASA was incapable of handing received data to a hardware buffer because the input rate exceeded the ASA capability to handle the data.
Ignored	This field is not used. The value is always 0.
Abort	This field is not used. The value is always 0.
L2 decode drops	The number of packets dropped because the name is not configured (**nameif** command) or a frame with an invalid VLAN id is received. On a standby interface in a redundant interface configuration, this counter may increase because this interface has no name (**nameif** command) configured.
Packets output	The number of packets sent on this interface.

Field	Description
Bytes	The number of bytes sent on this interface.
Underruns	The number of times that the transmitter ran faster than the ASA could handle.
Output Errors	The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.
Collisions	The number of messages retransmitted due to an Ethernet collision (single and multiple collisions). This usually occurs on an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once by the output packets.
Interface resets	The number of times an interface has been reset. If an interface is unable to transmit for three seconds, the ASA resets the interface to restart transmission. During this interval, connection state is maintained. An interface reset can also happen when an interface is looped back or shut down.
Babbles	Unused. (“babble” means that the transmitter has been on the interface longer than the time taken to transmit the largest frame.)
Late collisions	The number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait. If you get a late collision, a device is jumping in and trying to send the packet on the Ethernet while the ASA is partly finished sending the packet. The ASA does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks and Ethernet networks running beyond the specification.
Deferred	The number of frames that were deferred before transmission due to activity on the link.
input reset drops	Counts the number of packets dropped in the RX ring when a reset occurs.
output reset drops	Counts the number of packets dropped in the TX ring when a reset occurs.
Rate limit drops	(For 4GE SSM interfaces only) The number of packets dropped if you configured the interface at non-Gigabit speeds and attempted to transmit more than 10 Mbps or 100 Mbps, depending on configuration..
Lost carrier	The number of times the carrier signal was lost during transmission.
No carrier	Unused.

Field	Description
Input queue (curr/max packets):	The number of packets in the input queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue. Not available for Gigabit Ethernet interfaces.
Output queue (curr/max packets):	The number of packets in the output queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue.
input queue (blocks free curr/low)	The curr/low entry indicates the number of current and all-time-lowest available slots on the interface's Receive (input) descriptor ring. These are updated by the main CPU, so the all-time-lowest (until the interface statistics are cleared or the device is reloaded) watermarks are not highly accurate.
output queue (blocks free curr/low)	The curr/low entry indicates the number of current and all-time-lowest available slots on the interface's Transmit (output) descriptor rings. These are updated by the main CPU, so the all-time-lowest (until the interface statistics are cleared or the device is reloaded) watermarks are not highly accurate.
Traffic Statistics:	The number of packets received, transmitted, or dropped.
Packets input	The number of packets received and the number of bytes.
Packets output	The number of packets transmitted and the number of bytes.
Packets dropped	The number of packets dropped. Typically this counter increments for packets dropped on the accelerated security path (ASP), for example, if a packet is dropped due to an access list deny. See the **show asp drop** command for reasons for potential drops on an interface.
1 minute input rate	The number of packets received in packets/sec and bytes/sec over the last minute.
1 minute output rate	The number of packets transmitted in packets/sec and bytes/sec over the last minute.
1 minute drop rate	The number of packets dropped in packets/sec over the last minute.
5 minute input rate	The number of packets received in packets/sec and bytes/sec over the last 5 minutes.
5 minute output rate	The number of packets transmitted in packets/sec and bytes/sec over the last 5 minutes.
5 minute drop rate	The number of packets dropped in packets/sec over the last 5 minutes.

Field	Description
Redundancy Information:	For redundant interfaces, shows the member physical interfaces. The active interface has "(Active)" after the interface ID. If you have not yet assigned members, you see the following output: `Members unassigned`
Last switchover	For redundant interfaces, shows the last time the active interface failed over to the standby interface.

Examples

The following is sample output from the **show interface** command on the ASA 5505, which includes switch ports:

```
ciscoasa# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        MAC address 00d0.2bff.449f, MTU 1500
        IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
    Interface Ethernet0/0 "", is up, line protocol is up
      Hardware is 88E6095, BW 100 Mbps, DLY 1000 usec
            Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
            Available but not configured via nameif
            MAC address 00d0.2bfd.6ec5, MTU not set
            IP address unassigned
            407 packets input, 53587 bytes, 0 no buffer
            Received 103 broadcasts, 0 runts, 0 giants
            0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
            0 L2 decode drops
            43 switch ingress policy drops
            0 packets output, 0 bytes, 0 underruns
            0 output errors, 0 collisions, 0 interface resets
            0 babbles, 0 late collisions, 0 deferred
            0 lost carrier, 0 no carrier
            0 rate limit drops
            0 switch egress policy drops
```

Table 7-7 shows each field description for the **show interface** command for switch interfaces, such as those for the Firepower 1010 or ASA 5505. See Table 7-6 for fields that are also shown for the **show interface** command.

Table 6: show interface for Switch Interfaces Fields

Field	Description
switch ingress policy drops	This drop is usually seen when a port is not configured correctly. This drop is incremented when a packet cannot be successfully forwarded within switch ports as a result of the default or user configured switch port settings. The following configurations are the likely reasons for this drop: • The **nameif** command was not configured on the VLAN interface. **Note** For interfaces in the same VLAN, even if the **nameif** command was not configured, switching within the VLAN is successful, and this counter does not increment. • The VLAN is shut down. • An access port received an 802.1Q-tagged packet. • A trunk port received a tag that is not allowed or an untagged packet. • The ASA is connected to another Cisco device that has Ethernet keepalives. For example, Cisco IOS software uses Ethernet loopback packets to ensure interface health. This packet is not intended to be received by any other device; the health is ensured just by being able to send the packet. These types of packets are dropped at the switch port, and the counter increments.
switch egress policy drops	Not currently in use.

The following sample output from the **show interface** command for the Secure Firewall 3100 shows the FEC mode as auto using cl74-fc.

```
ciscoasa(config-if)# sh int eth1/5
Interface Ethernet1/5 "", is up, line protocol is up
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
   Full-Duplex(fullDuplex), 25000 Mbps(25gbps)
   Available but not configured via nameif
   MAC address fc58.9a06.9112, MTU not set
   IP address unassigned
   FEC mode is auto(cl74-fc)
   13 packets input, 2165 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   0 pause input, 0 resume input
   0 packets output, 0 bytes, 0 underruns
   0 pause output, 0 resume output
   0 output errors, 0 collisions, 0 interface resets
   0 late collisions, 0 deferred
   0 input reset drops, 0 output reset drops
```

Examples

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

```
ciscoasa# show interface detail
```

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

Table 7-7 shows each field description for the **show interface detail** command. See Table 7-7 for fields that are also shown for the **show interface** command.

Table 7: show interface detail Fields

Field	Description
Demux drops	(On Internal-Data interface only) The number of packets dropped because the ASA was unable to demultiplex packets from SSM interfaces. SSM interfaces communicate with the native interfaces across the backplane, and packets from all SSM interfaces are multiplexed on the backplane.
Control Point Interface States:	
Interface number	A number used for debugging that indicates in what order this interface was created, starting with 0.

Field	Description
Interface config status	The administrative state, as follows: • active—The interface is not shut down. • not active—The interface is shut down with the **shutdown** command.
Interface state	The actual state of the interface. In most cases, this state matches the config status above. If you configure high availability, it is possible there can be a mismatch because the ASA brings the interfaces up or down as needed.
Asymmetrical Routing Statistics:	
Received X1 packets	Number of ASR packets received on this interface.
Transmitted X2 packets	Number of ASR packets sent on this interfaces.
Dropped X3 packets	Number of ASR packets dropped on this interface. The packets might be dropped if the interface is down when trying to forward the packet.

The following is sample output from the **show interface detail** command on the ASA 5512-X through ASA 5555-X, which shows combined statistics for the Management 0/0 interface (shown as "Internal-Data0/1") for both the ASA and the software module. The output also shows the Internal-Control0/0 interface, which is used for control traffic between the software module and the ASA.

```
Interface Internal-Data0/1 "ipsmgmt", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "ipsmgmt":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active
```

```
Interface Internal-Control0/0 "cplane", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "cplane":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active
```

See the following output for **show interface detail** for the Secure Firewall 3100 showing the egress interface for a queue:

```
ciscoasa# show interface detail
Interface Internal Data0/1 "", is up, line protocol is up
   Hardware is , BW 500000 Mbps, DLY 1000 usec
      (Full duplex), (50000 Mbps)
      [...]
         TX[64]: 0 packets, 0 bytes, 0 underruns
            Blocks free curr /low: 511/512
            Used by Ethernet1/1
         TX[65]: 0 packets, 0 bytes, 0 underruns
            Blocks free curr /low: 511/512
            Used by Ethernet1/1
```

See the following output for the **show interface vni 1** command:

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
```

```
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
```

See the following output for the **show interface vni 1 summary** command:

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear interface	Clears counters for the **show interface** command.
delay	Changes the delay metric for an interface.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.

show interface ip brief

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

show interface [*physical_interface* [*.subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] **ip brief**

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabit ethernet0/1** . See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For models with a built-in switch, such as the ASA 5505 adaptive security appliance, specifies the VLAN interface.

Command Default

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	Support for VLAN interfaces and for the Management 0/0 interface or subinterface in transparent mode was added.
9.10(1)	Support for supervisor association for the Firepower 2100/4100/9300 devices was added.

Usage Guidelines

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

Note In ASA virtual (ASAv), the **show ip brief** output may display status of the line protocol as 'up', even when the interface is administratively down. This status does not imply any change in the functionality, namely, the packets are dropped when the interface is administratively down.

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

Examples

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

```
ciscoasa# show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   admin  down            down
    GigabitEthernet0/2         10.1.1.50       YES manual  admin down            down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    admin down            down
    Management0/0              209.165.201.3   YES CONFIG  up
The following is sample output from the show ip brief
command on ASA with FXOS:
ciscoasa# sh int ip br
Interface                  IP-Address      OK?           Method Status      Protocol
Internal-Data0/0           unassigned      YES           unset  up          up
Vlan10                     172.18.249.190  YES           CONFIG up          up
Vlan80                     80.1.1.1        YES           manual up          up
Vlan300                    14.30.1.1       YES           CONFIG up          up
....
Ethernet1/1                unassigned      YES           unset  up          up
Ethernet1/2                unassigned      YES           unset  down        down
Ethernet1/3                unassigned      unassociated  unset  admin down  down
Ethernet1/4                unassigned      unassociated  unset  admin down  down
Ethernet1/5                unassigned      YES           unset  up          up
Ethernet1/6                unassigned      unassociated  unset  down        down
Ethernet1/7                unassigned      unassociated  unset  down        down
Ethernet1/8                unassigned      unassociated  unset  up          up
Internal-Data1/1           169.254.1.1     YES           unset  up          up
Management1/1              unassigned      YES           unset  up          up
BVI50                      50.1.1.3        YES           CONFIG up          up
Port-channel3              unassigned      YES           unset  down        down
Port-channel8              8.0.0.1         YES           manual up          up
```

Examples

Table 7-7 shows each field description.

Table 8: show interface ip brief Fields

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command. If you show all interfaces, then information about the internal interface for the AIP SSM displays, if installed on the ASA. The internal interface is not user-configurable, and the information is for debugging purposes only.
IP-Address	The interface IP address.

Field	Description
OK?	This column displays "YES" if the interface is associated with supervisor; displays “unassociated” if the interface is not associated with supervisor. This state is applicable only for Firepower 2100/4100/9300 interfaces and devices. For FXOS-based ASA devices, this column displays “unassociated” when interfaces are added to the port channels. For other devices, this column is not currently used, and always shows “YES”.
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—Configured the running configuration. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.
Status	The administrative state, as follows: • up—The interface is not shut down. • admin down—The interface is shut down with the **shutdown** command. **Note** In ASA virtual (ASAv) platform, the status of the line protocol displays as up, even when the interface status is administratively down. This does not change the functionality-the packets are dropped when the interface is administratively down.
Protocol	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.

Related Commands

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

show inventory

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

show inventory *mod_id*

Syntax Description

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

Command Default

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

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was introduced.
8.4(2)	The output for an SSP was added. In addition, support for a dual SSP installation was added.
8.6(1)	The output for the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X (the chassis, redundant power supplies, and I/O expansion card) was added.
9.1(1)	The output for the ASA CX module was added.
9.24(1)	The output for field-replaceable memory module was added.

Usage Guidelines

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

The PID is the identifier used to order a product. Historically, it has also been called the “Product Name” or “Part Number.” Use the PID when ordering a replacement part. Along with PID, DC PSU data is also displayed.

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

The SN is the vendor-unique serialization of the product. Each manufactured product has a unique serial number assigned at the factory, which cannot be changed in the field. The serial number is the means by which

to identify an individual, specific instance of a product. The serial number can be different lengths for the various components of the device.

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

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

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



Note When two SSPs are installed in the same chassis, the number of the module indicates the physical location of the module in the chassis. The chassis master is always the SSP installed in slot 0. Only those sensors with which the SSP is associated are displayed in the output.The term *module* in the output is equivalent to physical slot. In the description of the SSP itself, the output includes module: 0 when it is installed in physical slot 0, and module: 1 otherwise. When the target SSP is the chassis master, the **show inventory** command output includes the power supplies and/or cooling fans. Otherwise, these components are omitted.

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

The output displays the field-replaceable memory modules installed on supported device. To improve the memory module identification, the output displays vendor, controller, channel information of the hardware and identifies the physical slot in which the memory module is installed. To improve the field serviceability, the output displays the operational status of the dual-inline memory modules.

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

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

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

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

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

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

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

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

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

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

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

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

Examples

The following is sample output from the **show inventory** command without any keywords or arguments. This sample output displays a list of Cisco entities installed in an ASA that are each assigned a PID, including a storage device used for an ASA CX module.

```
ciscoasa> show inventory

Name: "Chassis", DESCR: "ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt"
PID: ASA5555           , VID: V01     , SN: FGL170441BU
Name: "power supply 1", DESCR: "ASA 5545-X/5555-X AC Power Supply"
PID: ASA-PWR-AC        , VID: N/A     , SN: 2CS1AX
Name: "Storage Device 1", DESCR: "Micron 128 GB SSD MLC, Model Number: C400-MTFDDAC128MAM"
PID: N/A               , VID: N/A     , SN: MXA174201RR
```

The following example shows the output of the **show inventory** command on a chassis master for a dual SSP installation:

```
ciscoasa> show inventory

Name: "module 0", DESCR: "ASA 5585-X Security Services Processor-40 w 6GE,4 SFP+"
PID: ASA5585-SSP-40    , VID: V01     , SN: JAF1436ACLJ
Name: "Chassis", DESCR: "ASA 5585-X"
PID: ASA5585           , VID: V01     , SN: 123456789AB
Name: "fan", DESCR: "ASA 5585-X Fan Module"
PID: ASA5585-FAN       , VID: V01     , SN: POG1434000G
Name: "power supply 0", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC    , VID: V01     , SN: POG1434002K
```

This command only shows removable modules. Thus, though **show interface brief** in ASA shows all the SFP interfaces in EPM, the **show inventory** command in ASA would only show data for interfaces that have an SFP plugged in. The following example shows the output of the **show inventory** command on SFP interface that is plugged in:

```
ciscoasa> show inventory

Name: "Ethernet 1/13", DESCR: "h10g-acu1m"
PID: SFP-10G-AOC1M, VID: , SN: A4Z1942K0UC-B
```

The following is sample output from the **show inventory** commands for Secure Firewall 4200. Use **connect fxos** to run the FXOS CLI inventory commands for viewing inventory and PSU details.

```
firepower /chassis # show inventory detail
Chassis 1:
    Product Name: Cisco Firepower 4225 Security Appliance
    PID: FPR-4225
    VID: V00
    Vendor: Cisco Systems, Inc
    Model: FPR-4225
    Serial (SN): FHH2551P00R
    HW Revision: 0.1
```

```
firepower /chassis # show inventory psu detail
Chassis 1:
    PSU 1:
        Presence: Missing
        VID: Unknown
        Vendor: Unknown
        Serial (SN): Unknown
        HW Revision: 0

    PSU 2:
        Presence: Equipped
        VID: V00
        Vendor: Cisco Systems, Inc
        Serial (SN): DTM243305H8
        HW Revision: 0
```

The following example shows the output of the **show inventory** command on field-replaceable memory module installed on a supported device:

```
ciscoasa> show inventory
 Name: "DIMM P0 CHANNEL A", DESCR: "Samsung M321RYGA0PB0-CWMKH", Status: "operable"
PID: MEM-CSF6100-96GB, VID: N/A, SN: 80CE012343055A8F33
```

Table 7-9 describes the fields shown in the display.

Table 9: Field Descriptions for show inventory

Field	Description
Name	Physical name (text string) assigned to the Cisco entity. For example, console, SSP, or a simple component number (port or module number), such as "1," depending on the physical component naming syntax of the device. Equivalent to the entPhysicalName MIB variable in RFC 2737.
DESCR	Physical description of the Cisco entity that characterizes the object. Equivalent to the entPhysicalDesc MIB variable in RFC 2737.
Status	The operational status of the field-replaceable memory module supported devices.
PID	Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.
VID	Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.
SN	Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.

Related Commands

Command	Description
show diag	Displays diagnostic information about the controller, interface processor, and port adapters for a networking device.
show tech-support	Displays general information about the router when it reports a problem.
connect fxos	Connects FXOS from the ASA CLI

show ip address

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

show ip address [*physical_interface* [.*subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For models with a built-in switch, such as the ASA 5505 adaptive security appliance, specifies the VLAN interface.

Command Default

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

Command Modes

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

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

Command History

Release	Modification
7.2(1)	Support for VLAN interfaces was added.

Usage Guidelines

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

Examples

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

```
ciscoasa# show ip address
System IP Addresses:
Interface                Name         IP address      Subnet mask       Method
```

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

Table 7-7 shows each field description.

Table 10: show ip address Fields

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command.
Name	The interface name set with the **nameif** command.
IP address	The interface IP address.
Subnet mask	The IP address subnet mask.
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—Configured the running configuration. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.

Related Commands

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

show ip address dhcp

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

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

Syntax Description

interface_name	Identifies the interface name set with the **nameif** command.
lease	Shows information about the DHCP lease.
mapped_name	In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Identifies the interface ID, such as **gigabit ethernet0/1** . See the **interface** command for accepted values.
proxy	Shows proxy entries in the IPL table.
server	Shows server entries in the IPL table.
subinterface	Identifies an integer between 1 and 4294967293 designating a logical subinterface.
summary	Shows summary for the entry.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The **lease** and **server** keywords to accommodate the new server functionality were added.
7.2(1)	Support for VLAN interfaces and for the Management 0/0 interface or subinterface in transparent mode was added.
9.1(4)	The proxy and summary keywords to accommodate the new server functionality were added.

Usage Guidelines

See the “Examples” section for a description of the display output.

Examples

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

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

Table 7-7 shows each field description.

Table 11: show ip address dhcp lease Fields

Field	Description
Temp IP Addr	The IP address assigned to the interface.
Temp sub net mask	The subnet mask assigned to the interface.
DHCP Lease server	The DHCP server address.
state	The state of the DHCP lease, as follows: • Initial—The initialization state, where the ASA begins the process of acquiring a lease. This state is also shown when a lease ends or when a lease negotiation fails. • Selecting—The ASA is waiting to receive DHCPOFFER messages from one or more DHCP servers, so it can choose one. • Requesting—The ASA is waiting to hear back from the server to which it sent its request. • Purging—The ASA is removing the lease because the client has released the IP address or there was some other error. • Bound—The ASA has a valid lease and is operating normally. • Renewing—The ASA is trying to renew the lease. It regularly sends DHCPREQUEST messages to the current DHCP server, and waits for a reply. • Rebinding—The ASA failed to renew the lease with the original server, and now sends DHCPREQUEST messages until it gets a reply from any server or the lease ends. • Holddown—The ASA started the process to remove the lease. • Releasing—The ASA sends release messages to the server indicating that the IP address is no longer needed.

Field	Description
DHCP transaction id	A random number chosen by the client, used by the client and server to associate the request messages.
Lease	The length of time, specified by the DHCP server, that the interface can use this IP address.
Renewal	The length of time until the interface automatically attempts to renew this lease.
Rebind	The length of time until the ASA attempts to rebind to a DHCP server. Rebinding occurs if the ASA cannot communicate with the original DHCP server, and 87.5 percent of the lease time has expired. The ASA then attempts to contact any available DHCP server by broadcasting DHCP requests.
Temp default-gateway addr	The default gateway address supplied by the DHCP server.
Temp ip static route0	The default static route.
Next timer fires after	The number of seconds until the internal timer triggers.
Retry count	If the ASA is attempting to establish a lease, this field shows the number of times the ASA tried sending a DHCP message. For example, if the ASA is in the Selecting state, this value shows the number of times the ASA sent discover messages. If the ASA is in the Requesting state, this value shows the number of times the ASA sent request messages.
Client-ID	The client ID used in all communication with the server.
Proxy	Specifies if this interface is a proxy DHCP client for VPN clients, True or False.
Proxy Network	The requested network.
Hostname	The client hostname.

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

```
ciscoasa# show ip address outside dhcp server
   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

Table 7-12 shows each field description.

Table 12: show ip address dhcp server Fields

Field	Description
DHCP server	The DHCP server address from which this interface obtained a lease. The top entry (“ANY”) is the default server and is always present.
Leases	The number of leases obtained from the server. For an interface, the number of leases is typically 1. If the server is providing address for an interface that is running proxy for VPN, there will be several leases.
Offers	The number of offers from the server.
Requests	The number of requests sent to the server.
Acks	The number of acknowledgments received from the server.
Naks	The number of negative acknowledgments received from the server.
Declines	The number of declines received from the server.
Releases	The number of releases sent to the server.
Bad	The number of bad packets received from the server.
DNS0	The primary DNS server address obtained from the DHCP server.
DNS1	The secondary DNS server address obtained from the DHCP server.
WINS0	The primary WINS server address obtained from the DHCP server.
WINS1	The secondary WINS server address obtained from the DHCP server.
Subnet	The subnet address obtained from the DHCP server.
DNS Domain	The domain obtained from the DHCP server.

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address dhcp	Sets the interface to obtain an IP address from a DHCP server.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.
show ip address	Displays the IP addresses of interfaces.

show ip address pppoe

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

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

Syntax Description

interface_name	Identifies the interface name set with the **nameif** command.
mapped_name	In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For models with a built-in switch, such as the ASA 5505 adaptive security appliance, specifies the VLAN interface.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

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

Examples

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

```
ciscoasa# show ip address outside pppoe
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.

Command	Description
ip address ppoe	Sets the interface to obtain an IP address from a PPPoE server.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.
show ip address	Displays the IP addresses of interfaces.

show ip audit count

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

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

Syntax Description

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

Command Default

If you do not specify a keyword, this command shows the matches for all interfaces (**global**).

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To create an audit policy, use the **ip audit name** command, and to apply the policy, use the **ip audit interface** command.

Examples

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

```
ciscoasa# show ip audit count
IP AUDIT GLOBAL COUNTERS
1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
2003 I ICMP Redirect              0
```

```
2004 I ICMP Echo Request          10
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 I DNS Host Info              0
6051 I DNS Zone Xfer              0
6052 I DNS Zone Xfer High Port    0
6053 I DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0
IP AUDIT INTERFACE COUNTERS: inside
...
```

Related Commands

Command	Description
clear ip audit count	Clears the count of signature matches for an audit policy.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

show ip local pool

To display IPv4 address pool information, use the **show ip local pool** command in privileged EXEC mode.

show ip local pool interface *pool_name*

Syntax Description

pool_name	The name of the address pool. Enter ? to see a list of pools.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

Examples

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

```
ciscoasa# show ip local pool test-ipv4-pool

Begin           End             Mask            Free     Held     In use
10.100.10.10    10.100.10.254   255.255.255.0     245        0        0
Available Addresses:
10.100.10.10
10.100.10.11
10.100.10.12
10.100.10.13
10.100.10.14
10.100.10.15
10.100.10.16
... (remaining output redacted)...
```

Related Commands

Command	Description
ip local pool	Configures an IPv4 address pool.

show ip verify statistics

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

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

Syntax Description

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

Command Default

This command shows statistics for all interfaces.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

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

Related Commands

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

show ips

To show all available IPS virtual sensors that are configured on the AIP SSM, use the **show ips** command in privileged EXEC mode.

show ips [**detail**]

Syntax Description

detail	(Optional) Shows the sensor ID number as well as the name.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

In multiple context mode, this command shows all virtual sensors when entered in the system execution space, but only shows the virtual sensors assigned to the context in the context execution space. See the **allocate-ips** command to assign virtual sensors to contexts.

Virtual sensors are available in IPS Version 6.0 and above.

Examples

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

```
ciscoasa# show ips
Sensor name
------------
ips1
ips2
```

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

```
ciscoasa# show ips detail
Sensor name              Sensor ID
------------             ---------
ips1                     1
ips2                     2
```

Related Commands

Command	Description
allocate-ips	Assigns a virtual sensor to a security context.
ips	Diverts traffic to the AIP SSM.

show ipsec df-bit

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

show ipsec df-bit *interface*

Syntax Description

interface	Specifies an interface name.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

Examples

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

```
ciscoasa(config)# show
 ipsec df-bit inside
df-bit inside copy
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec df-bit	Configures the IPsec DF-bit policy for IPsec packets.
crypto ipsec fragmentation	Configures the fragmentation policy for IPsec packets.

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

show crypto ipsec fragmentation

To display the fragmentation policy for IPsec packets, use the **show ipsec fragmentation** command in global configuration or privileged EXEC mode. You can also use the command synonym **show crypto ipsec fragmentation**.

show ipsec fragmentation *interface*

Syntax Description

interface	Specifies an interface name.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

Examples

The following example, entered in global configuration mode, displays the IPsec fragmentation policy for an interface named inside:

```
ciscoasa(config)# show ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPsec packets.
crypto ipsec df-bit	Configures the DF-bit policy for IPsec packets.

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

show ipsec policy

To display IPsec secure socket API (SS API) security policy configured for OSPFv3, use the **show ipsec policy** command in global configuration or privileged EXEC mode. You can also use the alternate form of this command: **show crypto ipsec policy**.

show ipsec policy

Syntax Description

This command has no keywords or variables.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following example shows the OSPFv3 authentication and encryption policy.

```
ciscoasa# show ipsec policy

Crypto IPsec client security policy data
Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901234567890
Outbound ESP Auth Key:   12345678901234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 123456789012345678901234567890123456789012
Outbound ESP Cipher Key: 123456789012345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

Related Commands

Command	Description
ipv6 ospf encryption	Configures the authentication and encryption policy for OSPFv3.
show crypto sockets	Displays secure socket information.

Command	Description
show ipv6 ospf interface	Displays information about OSPFv3 interfaces.

show ipsec sa

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

show ipsec sa [**assigned-address** *hostname or IP address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for OSPFv3 and multiple context mode was added.
9.1(4)	Output has been updated to reflect the assigned IPv6 address and to indicate the GRE Transport Mode security association when doing IKEv2 dual traffic.

Examples

The following example, entered in global configuration mode, displays IPsec SAs, including the assigned IPv6 address and the Tansport Mode and GRE encapsulation indication.

```
ciscoasa(config)# sho ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23
      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 4
     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624
    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

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

```
ciscoasa(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
```

```
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3),}
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    Crypto map tag: def, local addr: 10.132.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```

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

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

```
ciscoasa(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
```

```
          slot: 0, conn_id: 3, crypto-map: def
          sa timing: remaining key lifetime (sec): 480
          IV size: 8 bytes
          replay detection support: Y
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

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

```
ciscoasa(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
```

```
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

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

```
ciscoasa(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
```

```
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

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

```
ciscoasa(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
```

```
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

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

```
ciscoasa(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

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

```
ciscoasa(config)# sho ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23
      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0      #TFC
rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 35
      local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624
    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config isakmp	Displays all the active ISAKMP configuration.

show ipsec sa summary

To display a summary of IPsec SAs, use the **show ipsec sa summary** command in global configuration mode or privileged EXEC mode.

show ipsec sa summary

Syntax Description

This command has no arguments or variables.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example, entered in global configuration mode, displays a summary of IPsec SAs by the following connection types:

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

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

```
Total           :    14
ciscoasa(config)#
```

Related Commands

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

show ipsec stats

To display a list of IPsec statistics, use the **show ipsec stats** command in global configuration mode or privileged EXEC mode.

show ipsec stats

Syntax Description

This command has no keywords or variables.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	ESPv3 statistics are shown with IPsec subsystems, and support for multiple context mode was added.

Usage Guidelines

The following table describes what the output entries indicate.

Output	Description
IPsec Global Statistics	This section pertains to the total number of IPsec tunnels that the ASA supports.
Active tunnels	The number of IPsec tunnels that are currently connected.
Previous tunnels	The number of IPsec tunnels that have been connected, including the active ones.
Inbound	This section pertains to inbound encrypted traffic that is received through IPsec tunnels.
Bytes	The number of bytes of encrypted traffic that has been received.

Output	Description
Decompressed bytes	The number of bytes of encrypted traffic that were received after decompression was performed, if applicable. This counter should always be equal to the previous one if compression is not enabled.
Packets	The number of encrypted IPsec packets that were received.
Dropped packets	The number of encrypted IPsec packets that were received and dropped because of errors.
Replay failures	The number of anti-replay failure that were detected on received, encrypted IPsec packets.
Authentications	The number of successful authentications performed on received, encrypted IPsec packets.
Authentication failures	The number of authentications failure detected on received, encrypted IPsec packets.
Decryptions	The number of successful decryptions performed on received, encrypted IPsec packets.
Decryption failures	The number of decryptions failures detected on received, encrypted IPsec packets.
Decapsulated fragments needing reassembly	The number of decryption IPsec packets that include IP fragments to be reassembled.
Outbound	This section pertains to outbound cleartext traffic to be transmitted through IPsec traffic.
Bytes	The number of bytes of cleartext traffic to be encrypted and transmitted through IPsec tunnels.
Uncompressed bytes	The number of bytes of uncompressed cleartext traffic to be encrypted and transmitted through IPsec tunnels. The counter should always be equal to the previous one if compression is not enabled
Packets	The number of cleartext packets to be encrypted and transmitted through IPsec tunnels.
Dropped packets	The number of cleartext packets to be encrypted and transmitted through IPsec tunnels that have been dropped because of errors.
Authentications	The number of successful authentications performed on packets to be transmitted through IPsec tunnels.
Authentication failures	The number of authentication failures that were detected on packets to be transmitted through IPsec tunnels.
Encryptions	The number of successful encryptions that were performed on packets to be transmitted through IPsec tunnels.

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

Examples

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

```
ciscoasa(config)# show ipsec stats
IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
 Fragmentation successes: 3
  Pre-fragmentation successes:2
  Post-fragmentation successes: 1
 Fragmentation failures: 2
  Pre-fragmentation failures:1
  Post-fragmentation failures: 1
 Fragments created: 10
 PMTUs sent: 1
 PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
```

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

```
ciscoasa# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 1
Previous tunnels: 1
Inbound
    Bytes: 93568
    Decompressed bytes: 0
    Packets: 86
    Dropped packets: 0
    Replay failures: 0
    Authentications: 0
    Authentication failures: 0
    Decryptions: 86
    Decryption failures: 0
    TFC Packets: 0
    Decapsulated fragments needing reassembly: 0
    Valid ICMP Errors rcvd: 0
```

```
    Invalid ICMP Errors rcvd: 0
Outbound
    Bytes: 93568
    Uncompressed bytes: 90472
    Packets: 86
    Dropped packets: 0
    Authentications: 0
    Authentication failures: 0
    Encryptions: 86
    Encryption failures: 0
    TFC Packets: 0
    Fragmentation successes: 0
        Pre-fragmentation successes: 0
        Post-fragmentation successes: 0
    Fragmentation failures: 0
        Pre-fragmentation failures: 0
        Post-fragmentation failures: 0
    Fragments created: 0
    PMTUs sent: 0
    PMTUs rcvd: 0
Offloaded Inbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Decryptions: 86
Offloaded Outbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Encryptions: 86
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
Inbound SA delete requests: 0
Outbound SA delete requests: 0
Inbound SA destroy calls: 0
Outbound SA destroy calls: 0
```

Related Commands

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