CHAPTER 49

show failover through show ipsec stats traffic Commands

show failover

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

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

Syntax Description

group	Displays the running state of the specified failover group.
history	Displays failover history. The failover history displays past failover state changes and the reason for the state change. History information is cleared with the device is rebooted.
interface	Displays failover and stateful link information.
num	Failover group number.
state	Displays the failover state of both failover units. The information displayed includes the primary or secondary status of the unit, the Active/Standby status of the unit, and the last reported reason for failover. The fail reason remains in the output even when the reason for failure is cleared.
statistics	Displays transmit and receive packet count of failover command interface.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
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 statitistics outpt includes information for the IPv6 neighbor discover table (IPv6 ND tbl) updates.

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 49-1 describes the interface states for failover.

Table 49-1 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.
Normal (Not-Monitored)	The interface is up but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
No Link	The physical link is down.
No Link (Waiting)	The physical link is down and the interface has not yet received a hello packet from the corresponding interface on the peer unit. After restoring the link, verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
No Link (Not-Monitored)	The physical link is down but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
Link Down	The physical link is up, but the interface is administratively down.
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.

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

Examples

The following is sample output from the **show failover** command for Active/Standby Failover. The ASAs are ASA 5500 series ASAs, each equipped with a CSC SSM as shown in the details for slot 1 of each ASA. The security appliances use IPv6 addresses on the failover link (folink) and the inside interface.

```
hostname# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
```

```
Failover unit Primary
Failover LAN Interface: folink Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.3/FE80::20d:29ff:fe1d:69f0): Normal
                  Interface outside (10.132.9.3): Normal
                  Interface folink (0.0.0.0/fe80::2a0:c9ff:fe03:101): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.3/24
                  CSC-SSM, 5.0 (Build#1176)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.4/FE80::20d:29ff:fe2b:7ba6): Normal
                  Interface outside (10.132.9.4): Normal
                  Interface folink (0.0.0.0/fe80::2e0:b6ff:fe07:3096): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.4/24
                  CSC-SSM, 5.0 (Build#1176)

Stateful Failover Logical Update Statistics
        Link : fover Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        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
       Route Session   165      0          70         6

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

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

```
hostname# 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-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
                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-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
                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 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 sample output from the **show failover state** command for an active-active setup:

```
hostname(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 sample output from the **show failover state** command for an active-standby setup:

```
hostname(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2009
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2009

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

Table 49-2 describes the output of the **show failover state** command.

Table 49-2 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. The following are possible configuration states for the active unit: • **Config Syncing**—Set on the active unit when it is performing a configuration synchronization to the standby unit. • **Interface Config Syncing** • **Sync Done**—Set when the active unit has completed a successful configuration synchronization to the standby unit. • **Ready for Config Sync**—Set on the active unit when the standby unit signals that it is ready to receive a configuration synchronization.
Communication State	Displays the status of the MAC address synchronization. • **Mac set**—The MAC addresses have been synchronized from the peer unit to this unit. • **Updated Mac**—Used when a MAC address is updated and needs to be synchronized to the other unit. Also used during the transition period where the unit is updating the local MAC addresses synchronized from the peer unit.
Date/Time	Displays a date and timestamp for the failure.
Last Failure Reason	Displays the reason for the last reported failure. This information is not cleared, even if the failure condition is cleared. This information changes only when a failover occurs. The following are possible fail reasons: • **Ifc Failure**—The number of interfaces that failed met the failover criteria and caused failover. • **Comm Failure**—The failover link failed or peer is down. • **Backplane Failure**
State	Displays the Primary/Secondary and Active/Standby status for the unit.
This host/Other host	This host indicates information for the device upon which the command was executed. Other host indicates information for the other device in the failover pair.

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

```
hostname(config)# show failover history
==========================================================================
Group     From State                 To State                   Reason
==========================================================================
. . .
03:42:29 UTC Apr 17 2009
    0     Sync Config                Failed
Backplane failed

03:42:29 UTC Apr 17 2009
    1     Standby Ready              Failed
Backplane failed

03:42:29 UTC Apr 17 2009
    2     Standby Ready              Failed
Backplane failed

03:44:39 UTC Apr 17 2009
    0     Failed                     Negotiation
Backplane operational

03:44:40 UTC Apr 17 2009
    1     Failed                     Negotiation
Backplane operational

03:44:40 UTC Apr 17 2009
    2     Failed                     Negotiation
Backplane operational

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

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.

Table 49-3 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 49-3 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.

Table 49-3 Failover States (continued)

States	Description
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.

```
hostname(config)# sh fail int
        interface folink GigabitEthernet0/2
                System IP Address: 2001:a0a:b00::a0a:b70/64
                My IP Address    : 2001:a0a:b00::a0a:b70
                Other IP Address : 2001:a0a:b00::a0a:b71
```

Related CommandsF

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

show failover exec

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **failover exec** command creates a session with the specified device. By default, that session is in global configuration mode. 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.

```
hostname(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.
hostname(config)# failover exec mate interface GigabitEthernet0/1
hostname(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.
hostname(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 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.2(1)	The capability to view information about partner application package files was added.

Examples

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

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

The following is sample output fromthe **show file info** command:

```
hostname# 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 firewall

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

show firewall

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# 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 firewall module version

To view the software version number of the ASA Services Module, enter the **show firewall module version** command in privileged EXEC mode.

show firewall switch {**1** | **2**} **module** [*module_number*] **version**

Syntax Description

module_number	(Optional) Specifies the module number.
switch {**1** | **2**}	Applies to VSS users only.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
Router# show firewall switch 1 module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

Related Commands

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

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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.1(1)	This command was introduced.
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:

```
hostname# 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.
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 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.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
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.

Examples

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

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

Related Commands

Command	Description
clear configure fragment	Clears the IP fragment reassembly configuration and resets the defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.

Command	Description
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show running-config fragment	Displays the IP fragment reassembly configuration.

show gc

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

show gc

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# show gc

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

Related Commands

Command	Description
clear gc	Removes the garbage collection process statistics.

show h225

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

show h225

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

This output indicates that there is currently 1 active H.323 call going through the 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
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the 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 signalling 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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.) Along with the **debug h323 h245 event**, **debug h323 h225 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

Examples

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

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

There is currently one H.245 control session active across the 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
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the 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 signalling connection or an H.323 control connection will be closed.

show h323-ras

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

show h323-ras

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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. Along with the **debug h323 ras event** and **show local-host** commands, this command is used for troubleshooting H.323 RAS inspection engine issues.

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

Examples

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

```
hostname# show h323-ras
Total: 1
 | GK | Caller
 | 172.30.254.214 10.130.56.14
hostname#
```

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
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.

Commands	Description
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 signalling connection or an H.323 control connection will be closed.

show history

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

show history

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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:

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

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

```
hostname# 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:

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

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

Related Commands

Command	Description
help	Displays help information for the command specified.

show icmp

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

show icmp

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was previously existing.

Usage Guidelines

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

Examples

The following example shows the ICMP configuration:

```
hostname# 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname# show idb
Maximum number of Software IDBs 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 49-4 shows each field description.

Table 49-4 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname#show igmp groups

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

Related Commands

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

show igmp interface

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

show igmp interface [*if_name*]

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
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:

```
hostname# show igmp interface inside

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

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# show igmp traffic

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

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

Related Commands

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

show import webvpn

To list the files, customization objects, translation tables, or plug-ins in flash memory that customize and localize the ASA or the AnyConnect Secure Mobility 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 AnyConnect 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 AnyConnect 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).

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
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.

Example

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

```
hostname# show import webvpn plug
ssh
rdp
vnc
hostname#

hostname#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
hostname# show import webvpn customization
Template
DfltCustomization
hostname#

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

hostname# show import webvpn url-list
Template
No bookmarks are currently defined
hostname#

hostname# show import webvpn webcontent
No custom webcontent is loaded
hostname#
```

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*] [**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 series adaptive security appliance. 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 **gigabitethernet 0/1**. See the **interface** command for accepted values.
redundant*number*	(Optional) Identifies the redundant interface ID, such as **redundant1**.
stats	(Default) Shows interface information and statistics. This keyword is the default, so this keyword is optional.
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.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
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)	This command added support for the 4GE SSM interfaces.
7.2(1)	This command added support for switch interfaces.

Release	Modification
8.0(2)	This command added support for redundant interfaces. 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)	This command added support for the ASA 5512-X through ASA 5555-X shared management interface and the control plane interface for the software module. 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.

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:

```
hostname# 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
```

Table 49-5 shows each field description.

Table 49-5 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.
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.

Table 49-5 show interface Fields (continued)

Field	Description

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.
MTU	The maximum size, in bytes, of packets allowed on this interface. If you do not set the interface name, this field shows “MTU not set.”
IP address	The interface IP address set using the **ip address** command or received from a DHCP server. In the system execution space, this field shows “IP address unassigned” because you cannot set the IP address in the system.
Subnet mask	The subnet mask for the IP address.
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.

Table 49-5 show interface Fields (continued)

Field	Description
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.
Packets output	The number of packets sent on this interface.
Bytes	The number of bytes sent on this interface.
Underruns	The number of times that the transmitter ran faster than the 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..

Table 49-5 show interface Fields (continued)

Field	Description
Lost carrier	The number of times the carrier signal was lost during transmission.
No carrier	Unused.
Input queue (curr/max packets):	The number of packets in the input queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue. Not available for Gigabit Ethernet interfaces.
Output queue (curr/max packets):	The number of packets in the output queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue.
input queue (blocks free curr/low)	The curr/low entry indicates the number of current and all-time-lowest available slots on the interface's Receive (input) descriptor ring. These are updated by the main CPU, so the all-time-lowest (until the interface statistics are cleared or the device is reloaded) watermarks are not highly accurate.
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.

Table 49-5 show interface Fields (continued)

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.

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

```
hostname# 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 49-7 shows each field description for the **show interface** command for switch interfaces, such as those for the ASA 5505 adaptive security appliance. See Table 49-6 for fields that are also shown for the **show interface** command.

Table 49-6 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 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:

```
hostname# 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 49-7 shows each field description for the **show interface detail** command. See Table 49-7 for fields that are also shown for the **show interface** command.

Table 49-7 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.
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
```

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 **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.

Defaults

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:

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

[1] Available for the Management 0/0 interface or subinterface only.

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command added support for VLAN interfaces, and for the Management 0/0 interface or subinterface in transparent mode.

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.

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

Examples

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

```
hostname# show interface ip brief
```

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

Table 49-7 shows each field description.

Table 49-8 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.
OK?	This column is not currently used, and always shows "Yes."
Method	The method by which the interface received the IP address. Values include the following: • 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. • administratively down—The interface is shut down with the **shutdown** command.
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), use the **show inventory** command in user EXEC or privileged EXEC mode.

show inventory *mod_id* [**slot**]

Syntax Description

mod_id	(Optional) Specifies the module ID.
slot	(Optional) Specifies the SSM slot number (the ASA is slot 0).

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Minor editorial changes.
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.

Usage Guidelines

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

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

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

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

The UDI refers to each product as an entity. Some entities, such as a chassis, have subentities 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.

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.

```
hostname# show inventory
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540           , VID:V01 , SN:P3000000998

Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20        , VID:V01 , SN:P0000000999

Name:"power supply", DESCR:"ASA 5500 Series 180W AC Power Supply"
PID:ASA-180W-PWR-AC   , VID:V01 , SN:123456789AB

hostname# show inventory 0
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540           , VID:V01 , SN:P3000000998

hostname# show inventory 1
Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20        , VID:V01 , SN:P0000000999
```

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

```
hostname(config)# 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
```

The following example shows the output of the **show inventory** command for an ASA CX module with a supported hard disk and a known model number:

```
hostname(config)# show inventory

Name: "Chassis", DESCR: "ASA 5555 Adaptive Security Appliance"
PID: ASA5555           , VID: V00     , SN: FCH1504V0D1

Name: "module 1", 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

Name: "power supply 0", DESCR: ""
PID:                   , VID: N/A     , SN:

Name: "power supply 1", DESCR: "ASA 5545-X/5555-X AC Power Supply"
PID: ASA-PWR-AC        , VID: N/A     , SN: 1341CH

Name: "Storage Device 1", DESCR: "Micron 128 GB SSD MLC, Model Number: C400-MTFDDAC128MAM"
PID: N/A               , VID: N/A     , SN: 1143034653F2
```

Table 49-9 describes the fields shown in the display.

Table 49-9 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.
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.

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.

Defaults

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:

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

Command History

Release	Modification
7.2(1)	This command added support for VLAN interfaces.

Usage Guidelines

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

Examples

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

```
hostname# show ip address
System IP Addresses:
Interface                Name         IP address      Subnet mask       Method
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 49-7 shows each field description.

Table 49-10 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 **gigabitethernet0/1**. 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.

Defaults

No default behavior or values.

Command Modes

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

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

[1] Available for the Management 0/0 interface or subinterface only.

Command History

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

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:

```
hostname# 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 49-7 shows each field description.

Table 49-11 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.
DHCP transaction id	A random number chosen by the client, used by the client and server to associate the request messages.

Table 49-11 show ip address dhcp lease Fields (continued)

Field	Description
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:

```
hostname# 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 49-12 shows each field description.

Table 49-12 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 acknowledgements received from the server.
Naks	The number of negative acknowledgements 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.

Defaults

No default behavior or values.

Command Modes

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

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

[1] Available for the Management 0/0 interface or subinterface only.

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname# show ip address outside pppoe
```

Related Commands

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

Defaults

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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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:

```
hostname# 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 verify statistics

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

show ip verify statistics [interface *interface_name*]

Syntax Description

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

Defaults

This command shows statistics for all interfaces.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

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

Related Commands

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

show 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

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:

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

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

```
hostname# 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 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) Dispay 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Added support for OSPFv3 and multiple context mode.
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.

```
hostname(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.

```
hostname(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

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

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #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)
hostname(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.

```
hostname(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

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

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

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

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

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

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

    Crypto map tag: def, local addr: 172.20.0.17

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

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

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

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

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

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

```
hostname(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

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

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

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

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

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

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

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

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

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

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

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

```
hostname(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

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

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

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

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

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

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

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

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

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

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

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
```

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

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

```
hostname(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

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

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

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

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

    Crypto map tag: def, local addr: 172.20.0.17

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

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

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

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

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

```
hostname(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

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

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

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

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

    Crypto map tag: def, local addr: 172.20.0.17

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

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

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

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

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

```
hostname(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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
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

```
hostname(config)# show ipsec sa summary

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

Related Commands

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

show ipsec stats

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

show ipsec stats

Syntax Description

This command has no keywords or variables.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
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.
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.

Output (continued)	Description (continued)
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.
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.

Output (continued)	Description (continued)
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:

```
hostname(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
```

```
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    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
hostname(config)#
```

Related Commands

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