CHAPTER 26

show isakmp ipsec-over-tcp stats through show route Commands

show isakmp ipsec-over-tcp stats

To display runtime statistics for IPsec over TCP, use the **show isakmp ipsec-over tcp stats** command in global configuration mode or privileged EXEC mode.

show isakmp ipsec-over-tcp stats

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
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp ipsec-over-tcp stats** command was introduced.
7.2(1)	The **show isakmp ipsec-over-tcp stats** command was deprecated. The **show crypto isakmp ipsec-over-tcp stats** command replaces it.

Usage Guidelines

The output from this command includes the following fields:

- Embryonic connections
- Active connections
- Previous connections
- Inbound packets
- Inbound dropped packets
- Outbound packets
- Outbound dropped packets
- RST packets
- Received ACK heart-beat packets
- Bad headers
- Bad trailers
- Timer failures

- Checksum errors
- Internal errors

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
hostname(config)# show isakmp ipsec-over-tcp stats
Global IPSec over TCP Statistics
--------------------------------
Embryonic connections: 2
Active connections: 132
Previous connections: 146
Inbound packets: 6000
Inbound dropped packets: 30
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 260
Received ACK heart-beat packets: 10
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
hostname(config)#
```

Related Commands

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

show isakmp sa

To display the IKE runtime SA database, use the **show isakmp sa** command in global configuration mode or privileged EXEC mode.

show isakmp sa [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

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)	The **show isakmp sa** command was introduced.
7.2(1)	This command was deprecated. The **show crypto isakmp sa** command replaces it.

Usage Guidelines

The output from this command includes the following fields:

Detail not specified.

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```
hostname(config)# show isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

hostname(config)#
```

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 adaptive security appliance.
show running-config isakmp	Displays all the active ISAKMP configuration.

show isakmp stats

To display runtime statistics, use the **show isakmp stats** command in global configuration mode or privileged EXEC mode.

show isakmp stats

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
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp stats** command was introduced.
7.2(1)	This command was deprecated. The **show crypto isakmp stats** command replaces it.

Usage Guidelines

Each one of the counters maps to an associated cikePhase1GW counter. For details on each of these counters, refer to CISCO-IPSEC-FLOW-MONITOR-MIB.my.

- Active/Standby Tunnels—cikePhase1GWActiveTunnels
- Previous Tunnels—cikePhase1GWPreviousTunnels
- In Octets—cikePhase1GWInOctets
- In Packets—cikePhase1GWInPkts
- In Drop Packets—cikePhase1GWInDropPkts
- In Notifys—cikePhase1GWInNotifys
- In P2 Exchanges—cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids—cikePhase1GWInP2ExchgInvalids
- In P2 Exchange Rejects—cikePhase1GWInP2ExchgRejects
- In P2 Sa Delete Requests—cikePhase1GWInP2SaDelRequests
- Out Octets—cikePhase1GWOutOctets
- Out Packets—cikePhase1GWOutPkts

- Out Drop Packets—cikePhase1GWOutDropPkts
- Out Notifys—cikePhase1GWOutNotifys
- Out P2 Exchanges—cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids—cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects—cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests—cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels—cikePhase1GWInitTunnels
- Initiator Fails—cikePhase1GWInitTunnelFails
- Responder Fails—cikePhase1GWRespTunnelFails
- System Capacity Fails—cikePhase1GWSysCapFails
- Auth Fails—cikePhase1GWAuthFails
- Decrypt Fails—cikePhase1GWDecryptFails
- Hash Valid Fails—cikePhase1GWHashValidFails
- No Sa Fails—cikePhase1GWNoSaFails

The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails

- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
hostname(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

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 adaptive security appliance.
show running-config isakmp	Displays all the active ISAKMP configuration.

show kernel process

To display the current status of the active kernel processes running on the security appliance, use the **show kernel process** command in privileged EXEC mode.

show kernel process

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(0)	This command was introduced.

Usage Guidelines

Use the show kernel process command to troubleshoot issues with the kernel running on the security appliance.

The output from the show kernel process command is lined up in the console output.

Examples

The following example displays output from the show kernel process command:

```
hostname# show kernel process

PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
  5    1  20 -5          0        0 3725736671    S        0 kthread
  7    5  10 -5          0        0 3725736671    S        0 kblockd/0
  8    5  20 -5          0        0 3726794334    S        0 kseriod
 66    5  20  0          0        0 3725811768    S        0 pdflush
 67    5  15  0          0        0 3725811768    S        0 pdflush
 68    1  15  0          0        0 3725824451    S        2 kswapd0
 69    5  20 -5          0        0 3725736671    S        0 aio/0
171    1  16  0     991232       80 3725684979    S        0 init
172  171  19  0     983040      268 3725684979    S        0 rcS
201  172  21  0    1351680      344 3725712932    S        0 lina_monitor
202  201  16  0 1017602048   899932 3725716348    S      212 lina
203  202  16  0 1017602048   899932          0    S        0 lina
204  203  15  0 1017602048   899932          0    S        0 lina
205  203  15  0 1017602048   899932 3725712932    S        6 lina
206  203  25  0 1017602048   899932          0    R 13069390 lina
```

```
hostname#
```

Table 26-1shows each field description.

Table 26-1 show kernel process Fields

Field	Description
PID	The process ID.
PPID	The parent process ID.
PRI	The priority of the process.
NI	The nice value, which is used in priority computation. The values range from 19 (nicest) to -19 (not nice to others),
VSIZE	The virtual memory size in bytes.
RSS	The resident set size of the process, in kilobytes.
WCHAN	The channel in which the process is waiting.
STAT	The state of the process: • R—Running • S—Sleeping in an interruptible wait • D—Waiting in an uninterruptible disk sleep • Z—zombie • T—Traced or stopped (on a signal) • P—Paging
RUNTIME	The number of jiffies that the process has been scheduled in user mode and kernel mode. The runtime is the sum of utime and stime.
COMMAND	The process name.

show local-host

To display the network states of local hosts, use the **show local-host** command in privileged EXEC mode.

show local-host | include interface [*ip_address*] [**detail**] [**all**][**brief**] **[connection {tcp <start>[-<end>] | udp <start>[-<end>] | embryonic <start>[-<end>]}]**

Syntax Description

all	(Optional) Includes local hosts connecting to the adaptive security appliance and from the adaptive security appliance.
brief	(Optional) Displays brief informationon local hosts.
connection	(Optional) Displays three typs of filters based on the number and type of connetcions: tcp, udp and embryonic. These filters can be used individually or jointly.
detail	(Optional) Displays the detailed network states of local host information, including more information about active xlates and network connections.
include interface	Specifies the IP addresses being used on each interface.
ip_address	(Optional) Specifies the local host IP address.

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
7.2(1)	For models with host limits, this command now shows which interface is considered to be the outside interface.
7.2(4)	Two new options, *connection* and *brief*, were added to the **show local-host** command so that the output is filtered by the number of connections for the inside hosts.

Usage Guidelines

The **show local-host** command lets you display the network states of local hosts. A local-host is created for any host that forwards traffic to, or through, the adaptive security appliance.

This command lets you show the translation and connection slots for the local hosts. This command provides information for hosts that are configured with the **nat 0 access-list** command when normal translation and connection states may not apply.

This command also displays the connection limit values. If a connection limit is not set, the value displays as 0 and the limit is not applied.

For models with host limits, In routed mode, hosts on the inside (Work and Home zones) count towards the limit only when they communicate with the outside (Internet zone). Internet hosts are not counted towards the limit. Hosts that initiate traffic between Work and Home are also not counted towards the limit. The interface associated with the default route is considered to be the Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit.

In the event of a SYN attack (with TCP intercept configured), the **show local-host** command output includes the number of intercepted connections in the usage count. This field typically displays only full open connections.

In the **show local-host** command output, the `TCP embryonic count to host counter` is used when a maximum embryonic limit (TCP intercept watermark) is configured for a host using a static connection. This counter shows the total embryonic connections to the host from other hosts. If this total exceeds the maximum configured limit, TCP intercept is applied to new connections to the host.

Examples

The following sample output is displayed by the **show local-host** command:

```
hostname# show local-host
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 1 active, 2 maximum active, 0 denied
```

The following sample output is displayed by the **show local-host** command on a adaptive security appliance with host limits:

```
hostname# show local-host
Detected interface 'outside' as the Internet interface. Host limit applies to all other
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
```

The following sample output is displayed by the **show local-host** command on a adaptive security appliance with host limits, but without a default route, the host limits apply to all interfaces. The default route interface might not be detected if the default route or the interface that the route uses is down.

```
hostname# show local-host
Unable to determine Internet interface from default route. Host limit applied to all
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

The following sample output is displayed by the **show local-host** command on a adaptive security appliance with unlimited hosts:

```
hostname# show local-host
Licensed host limit: Unlimited

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

The following examples show how to display the network states of local hosts:

```
hostname# show local-host all
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464

hostname# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

hostname# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
```

```
Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active, 1
maximum active, 0 denied
```

The following example shows all hosts who have at least four udp connections and have between one to 10 tcp connections at the same time:

```
hostname# show local-host connection udp 4 tcp 1-10
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
        TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
        watermark = unlimited UDP flow count/limit = 4/unlimited
Xlate:
        Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
        10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
        10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
        maximum active, 0 denied
```

The following example shows local-host addresses and connection counters using the **brief** option:

```
hostname# show local-host connection udp 2
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
        TCP flow count/limit = 1/unlimited
        TCP embryonic count to host = 0
        TCP intercept watermark = unlimited UDP flow count/limit = 4/unlimited
Interface OUTSIDE: 3 active, 5 maximum active, 0 denied
```

The following examples shows the output when using the *brief* and *connection* syntax:

```
hostname#show local-host brief
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied

hostname# show local-host connection
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied
```

Related Commands

Command	Description
clear local-host	Releases network connections from local hosts displayed by the **show local-host** command.
nat	Associates a network with a pool of global IP addresses.

show logging

To show the logs in the buffer or other logging settings, use the **show logging** command in privileged EXEC mode.

show logging [**message** [*syslog_id* | **all**] | **asdm** | **queue** | **setting**]

Syntax Description

all	(Optional) Displays all syslog message IDs, along with whether they are enabled or disabled.
asdm	(Optional) Displays ASDM logging buffer content.
message	(Optional) Displays messages that are at a non-default level. See the **logging message** command to set the message level.
queue	(Optional) Displays the syslog message queue.
setting	(Optional) Displays the logging setting, without displaying the logging buffer.
syslog_id	(Optional) Specifies a message number to display.

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.
8.0(2)	Indicates whether a syslog server is configured to use an SSL/TLS connection.

Usage Guidelines

If the **logging buffered** command is in use, the **show logging** command without any keywords shows the current message buffer and the current settings.

The **show logging queue** command allows you to display the following:

- Number of messages that are in the queue
- Highest number of messages recorded that are in the queue
- Number of messages that are discarded because block memory was not available to process them

Note Zero is an acceptable number for the configured queue size and represents the maximum queue size allowed. The output for the **show logging queue** command will display the actual queue size if the the configured queue size is zero.

Examples

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

```
hostname(config)# show logging
Syslog logging: enabled
    Timestamp logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 37 messages logged
    Trap logging: disabled
305001: Portmapped translation built for gaddr 209.165.201.5/0 laddr 192.168.1.2/256
...
```

The following is sample output from the **show logging** command with a secure syslog server configured:

```
hostname(config)# logging host inside 10.0.0.1 TCP/1500 secure
hostname(config)# show logging
Syslog logging: disabled
    Facility:
    Timestamp logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level debugging, 135 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: list show _syslog, facility, 20, 21 messages logged
        Logging to inside 10.0.0.1 tcp/1500 SECURE
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging disabled
```

The following is sample output from the **show logging message all** command:

```
hostname(config)# show logging message all

syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

Related Commands

Command	Description
logging asdm	Enables logging to ASDM
logging buffered	Enables logging to the buffer.
logging host	Defines a syslog server.
logging message	Sets the message level or disables messages.
logging queue	Configures the logging queue.

show logging flow-export-syslogs

To display all of the syslog messages whose information is also captured by NetFlow and that will be affected by the **logging flow-export-syslogs enable | disable** commands, use the **show logging flow-export-syslogs** command in privileged EXEC mode.

show logging flow-export-syslogs

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.

Usage Guidelines

After you enter the **logging flow-export syslogs disable** command, make sure that you know which syslog messages have been disabled. The disabled syslog messages are as follows:

Syslog Message	Description
106015	A TCP flow was denied because the first packet was not a SYN packet.
106023	A flow that is denied by an ingress ACL or an egress ACL that is attached to an interface through the **access-group** command.
106100	A flow that is permitted or denied by an ACL.
302013 and 302014	A TCP connection and deletion.
302015 and 302016	A UDP connection and deletion.
302017 and 302018	A GRE connection and deletion.
302020 and 302021	An ICMP connection and deletion.
313001	An ICMP packet to the security appliance was denied.
313008	An ICMPv6 packet to the security appliance was denied.
710003	An attempt to connect to the security appliance was denied.

Examples

The following is sample output from the **show logging flow-export-syslogs** command, which lists the syslog messages that will be disabled:

```
hostname(config)# show logging flow-export-syslogs

Syslog ID          Type                 Status
302013           Flow Created          Enabled
302015           Flow Created          Enabled
302017           Flow Created          Enabled
302020           Flow Created          Enabled
302014           Flow Deleted          Enabled
302016           Flow Deleted          Enabled
302018           Flow Deleted          Enabled
302021           Flow Deleted          Enabled
106015           Flow Denied           Enabled
106023           Flow Denied           Enabled
313001           Flow Denied           Enabled
313008           Flow Denied           Enabled
710003           Flow Denied           Enabled
106100           Flow Created/Denied   Enabled
```

Related Commands

Commands	Description
flow-export destination *interface-name ipv4-address | hostname udp-port*	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 *minutes*	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

show logging rate-limit

To display disallowed syslog messages, use the **show logging rate-limit** command in privileged EXEC mode.

show logging rate-limit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Examples

The following example shows sample output from the **show logging rate-limit** command:

```
hostname(config)# show logging rate-limit
%ASA-7-710005: TCP request discarded from 171.69.39.0/2678 to management:10.89.130.244/443
%ASA-7-711002: Task ran for 27 msec, Process = ssm_mgmt_ifc_poll_thread, PC = 896fcac,
Traceback =
%ASA-7-711002: Task ran for 27 msec, Process = ssm_mgmt_ifc_poll_thread, PC = 896fcac,
Traceback =   0x0807C0FA
%ASA-6-106015: Deny TCP (no connection) from 171.69.39.0/2685 to 10.89.130.244/443 flags
FIN PSH ACK  on interface management
%ASA-7-710005: TCP request discarded from 171.69.39.0/2685 to management:10.89.130.244/443
%ASA-6-302013: Built inbound TCP connection 2116 for management:171.69.39.0/2689
(171.69.39.0/2689) to identity:10.89.130.244/443 (10.89.130.244/443)
%ASA-6-725001: Starting SSL handshake with client management:171.69.39.0/2689 for TLSv1
session.
%ASA-6-725003: SSL client management:171.69.39.0/2689 request to resume previous session.
%ASA-6-725002: Device completed SSL handshake with client management:171.69.39.0/2689
%ASA-6-605005: Login permitted from 171.69.39.0/2689 to management:10.89.130.244/https for
user "enable_15"
%ASA-5-111007: Begin configuration: 171.69.39.0 reading from http [POST]
```

Related Commands

Command	Description
show logging	Displays the enabled logging options.

show mac-address-table

To show the MAC address table, use the **show mac-address-table** command in privileged EXEC mode.

show mac-address-table [*interface_name* | **count** | **static**]

Syntax Description

count	(Optional) Lists the total number of dynamic and static entries.
interface_name	(Optional) Identifies the interface name for which you want to view MAC address table entries.
static	(Optional) Lists only static entries.

Defaults

If you do not specify an interface, all interface MAC address entries are shown.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show mac-address-table** command:

```
hostname# show mac-address-table
interface          mac address       type      Time Left
------------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

The following is sample output from the **show mac-address-table** command for the inside interface:

```
hostname# show mac-address-table inside
interface          mac address       type      Time Left
------------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

The following is sample output from the **show mac-address-table count** command:

```
hostname# show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-address-table static	Adds a static MAC address entry to the MAC address table.
mac-learn	Disables MAC address learning.

show management-access

To display the name of the internal interface configured for management access, use the show management-access command in privileged EXEC mode.

show management-access

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
Preexisting	This command was preexisting.

Usage Guidelines

The **management-access** command lets you define an internal management interface using the IP address of the firewall interface specified in *mgmt_if*. (The interface names are defined by the **nameif** command and displayed in quotes, " ", in the output of the **show interface** command.)

Examples

The following example shows how to configure a firewall interface named "inside" as the management access interface and display the result:

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

Related Commands

Command	Description
clear configure management-access	Removes the configuration of an internal interface for management access of the adaptive security appliance.
management-access	Configures an internal interface for management access.

show memory

To display a summary of the maximum physical memory and current free memory available to the operating system, use the **show memory** command in privileged EXEC mode.

show memory [**detail**]

Note On both the ASA 5580-20 and the ASA 5580-40 adaptive security appliances only 4GB of memory is available for features. The rest are reserved or used by the OS. The show memory command will only display values relative to 4GB.

Syntax Description

detail	(Optional) Displays a detailed view of free and allocated system memory.

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
Preexisting	This command was preexisting.

Usage Guidelines

The **show memory** command lets you display a summary of the maximum physical memory and current free memory available to the operating system. Memory is allocated as needed.

You can use the **`show memory detail`** output with **`show memory binsize`** command to debug memory leaks.

The **show memory detail** command output can be broken down into three sections: Summary, DMA Memory, and HEAP Memory. The summary displays how the total memory is allocated. Memory that is not tied to DMA or reserved is considered the HEAP. The memory labeled Free Memory is the unused memory in the HEAP. The Allocated memory in use value is how much of the HEAP has been allocated. The break down of HEAP allocation is displayed later in the output. Reserved memory and DMA Reserved memory are used by different system processes and primarily VPN services.

You can also display the information from the **show memory** command using SNMP.

Examples

This example shows how to display a summary of the maximum physical memory and current free memory available:

```
hostname# show memory
Free memory:       845044716 bytes (79%)
Used memory:       228697108 bytes (21%)
-------------     ----------------
Total memory:     1073741824 bytes (100%)
```

This example shows detailed memory output:

```
hostname# show memory detail
Free memory:                          130546920 bytes (49%)
Used memory:                          137888536 bytes (51%)
    Allocated memory in use:           33030808 bytes (12%)
    Reserved memory:                       65454208 bytes (24%)
    DMA Reserved memory:                   39403520 bytes (15%)
    ----------------------------      ----------------
Total memory:                         268435456 bytes (100%)
Dynamic Shared Objects(DSO):              0 bytes
DMA memory:
    Unused memory:                    3212128 bytes ( 8%)
    Crypto reserved memory:           2646136 bytes ( 7%)
        Crypto free:                  1605536 bytes ( 4%)
        Crypto used:                  1040600 bytes ( 3%)
    Block reserved memory:            33366816 bytes (85%)
        Block free:                   31867488 bytes (81%)
        Block used:                   1499328 bytes ( 4%)
    Used memory:                       178440 bytes ( 0%)
    ----------------------------      ----------------
    Total memory:                     39403520 bytes (100%)
    HEAP memory:
        Free memory:                  130546920 bytes (80%)
        Used memory:                  33030808 bytes (20%)
            Init used memory by library:  4218752 bytes ( 3%)
            Allocated memory:         28812056 bytes (18%)
    ----------------------------      ----------------
    Total memory:                     163577728 bytes (100%)

Least free memory:     122963528 bytes (75%)
Most used memory:      40614200 bytes (25%)

    ----- fragmented memory statistics -----

fragment size      count       total
    (bytes)                   (bytes)
---------------- ---------- --------------
        16         113        1808


<output omitted>
```

Related Commands

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the adaptive security appliance.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.

show memory app-cache

To to observe memory usage by application, use the **show memory app-cache** command in privileged EXEC mode.

show memory app-cache [**threat-detection | host | flow | tcb | http | access-list]** [**detail**]

Syntax Descriptions

access-list	(Optional) Shows the application level memory cache for access-list.
detail	(Optional) Shows a detailed view of free and allocated system memory.
flow	(Optional) Shows the application level memory cache for flow.
host	(Optional) Shows application level memory cache for host.
http	(Optional) Shows application level memory cache for http.
tcb	(Optional) Shows application level memory cache for tcb.
threat-detection	(Optional) Shows application level memory cache for threat-detetcion.

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(1)	This command was introduced.
8.1(1)	The *access list* and *http* options were added.

Usage Guidelines

This command provides a better a way to observe memory usage by application.

Examples

This example shows how to display the out put for :

```
hostname(config)# sh mem app-cache threat-detection
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168

hostname(config)# sh mem app-cache threat-detection detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
TD ACE stats 50 0 2 0 1936
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
```

```
TD Host/Port counte 100 0 2 0 48
TD Host stats 50 50 16120 0 116515360
TD Subnet stats 50 2 113 0 207016
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168

hostname(config)# sh mem app-cache host d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Host Core 0 1000 1000 5116 0 961808
SNP Host Core 1 1000 1000 4968 0 933984
SNP Host Core 2 1000 1000 5413 0 1017644
SNP Host Core 3 1000 1000 4573 0 859724

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 20070 0 3773160

hostname(config)# sh mem app-cache flow d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn Core 0 1000 1000 893 0 639388
SNP Conn Core 1 1000 948 980 0 701680
SNP Conn Core 2 1000 1000 1175 0 841300
SNP Conn Core 3 1000 1000 901 0 645116

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 3948 3949 0 2827484

hostname(config)# sh mem app-cache access-list d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
NP ACL log c Core 0 1000 0 1 0 68
NP ACL log c Core 1 1000 0 6 0 408
NP ACL log c Core 2 1000 0 19 0 1292
NP ACL log c Core 3 1000 0 0 0 0
NP ACL log f Core 0 1000 0 0 0 0
NP ACL log f Core 1 1000 0 0 0 0
NP ACL log f Core 2 1000 0 0 0 0
NP ACL log f Core 3 1000 0 0 0 0

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 26 0 1768

hostname(config)# sh mem app-cache http d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
Inspect HTTP Core 0 1000 0 0 0 0
Inspect HTTP Core 1 1000 0 0 0 0
Inspect HTTP Core 2 1000 0 0 0 0
Inspect HTTP Core 3 1000 0 0 0 0
HTTP Result Core 0 1000 0 0 0 0
HTTP Result Core 1 1000 0 0 0 0
HTTP Result Core 2 1000 0 0 0 0
HTTP Result Core 3 1000 0 0 0 0

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 0 0 0

hostname(config)# sh mem app-cache tcb d
```

```
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB Core 0 1000 1000 968 0 197472
SNP TCB Core 1 1000 1000 694 0 141576
SNP TCB Core 2 1000 1000 1304 0 266016
SNP TCB Core 3 1000 1000 1034 0 210936

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 4000 0 816000
```

Related Commands

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the security appliance.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.
show memory	Displays a summary of the maximum physical memory and current free memory available to the operating system.

show memory binsize

To display summary information about the chunks allocated for a specific bin size, use the **show memory binsize** command in privileged EXEC mode.

show memory binsize *size*

Syntax Description

size	Displays chunks (memory blocks) of a specific bin size. The bin size is from the "fragment size" column of the **show memory detail** command output.

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

This command has no usage guidelines.

Examples

The following example displays summary information about a chunk allocated to a bin size of 500:

```
hostname# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

Related Commands

Command	Description
show memory-caller address	Displays the address ranges configured on the adaptive security appliance.
show memory profile	Displays information about the memory usage (profiling) of the adaptive security appliance.
show memory	Displays a summary of the maximum physical memory and current free memory available to the operating system.

show memory delayed-free-poisoner

To display a summary of the **memory delayed-free-poisoner** queue usage, use the **show memory delayed-free-poisoner** command in privileged EXEC mode.

show memory delayed-free-poisoner

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **clear memory delayed-free-poisoner** command to clear the queue and statistics.

Examples

This following is sample output from the **show memory delayed-free-poisoner** command:

```
hostname# show memory delayed-free-poisoner
delayed-free-poisoner statistics:
         3335600:  memory held in queue
            6095:  current queue count
               0:  elements dequeued
               3:  frees ignored by size
            1530:  frees ignored by locking
              27:  successful validate runs
               0:  aborted validate runs
        01:09:36:  local time of last validate
```

Table 26-2 describes the significant fields in the **show memory delayed-free-poisoner** command output.

Table 26-2 **show memory delayed-free-poisoner** Command Output Descriptions

Field	Description
memory held in queue	The memory that is held in the delayed free-memory poisoner tool queue. Such memory is normally in the "Free" quantity in the **show memory** output if the delayed free-memory poisoner tool is not enabled.
current queue count	The number of elements in the queue.
elements dequeued	The number of elements that have been removed from the queue. This number begins to increase when most or all of the otherwise free memory in the system ends up in being held in the queue.
frees ignored by size	The number of free requests not placed into the queue because the request was too small to hold required tracking information.
frees ignored by locking	The number of free requests intercepted by the tool not placed into the queue because the memory is in use by more than one application. The last application to free the memory back to the system ends up placing such memory regions into the queue.
successful validate runs	The number of times since monitoring was enabled or cleared using the **clear memory delayed-free-poisoner** command that the queue contents were validated (either automatically or by the **memory delayed-free-poisoner validate** command).
aborted validate runs	The number of times since monitoring was enabled or cleared using the **clear memory delayed-free-poisoner** command that requests to check the queue contents have been aborted because more than one task (either the periodic run or a validate request from the CLI) attempted to use the queue at a time.
local time of last validate	The local system time when the last validate run completed.

Related Commands

Command	Description
clear memory delayed-free-poisoner	Clears the delayed free-memory poisoner tool queue and statistics.
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
memory delayed-free-poisoner validate	Forces validation of the elements in the delayed free-memory poisoner tool queue.

show memory profile

To display information about the memory usage (profiling) of the adaptive security appliance, use the **show memory profile** command in privileged EXEC mode.

show memory profile [peak] [detail | collated | status]

Syntax Description

collated	(Optional) Collates the memory information displayed.
detail	(Optional) Displays detailed memory information.
peak	(Optional) Displays the peak capture buffer rather than the "in use" buffer.
status	(Optional) Displays the current state of memory profiling and the peak capture buffer.

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

Use the **show memory profile** command to troubleshoot memory usage level and memory leaks. You can still see the profile buffer contents even if profiling has been stopped. Starting profiling clears the buffer automatically.

Note The adaptive security appliance might experience a temporary reduction in performance when memory profiling is enabled.

Examples

The following example shows...

```
hostname# show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

The output of the **show memory profile detail** command is divided into six data columns and one header column, at the far left. The address of the memory bucket corresponding to the first data column is given at the header column (the hexidecimal number). The data itself is the number of bytes that is

held by the text/code that falls in the bucket address. A period (.) in the data column means no memory is held by the text at this bucket. Other columns in the row correspond to the bucket address that is greater than the increment amount from the previous column. For example, the address bucket of the first data column in the first row is 0x001069e0. The address bucket of the second data column in the first row is 0x001069e4 and so on. Normally the header column address is the next bucket address; that is, the address of the last data column of the previous row plus the increment. All rows without any usage are suppressed. More than one such contiguous row can be suppressed, indicated with three periods at the header column (...).

```
hostname# show memory profile detail
Range: start = 0x08048000, end = 0x089d1680, increment = 00000004
Total =       9770
  ...
0x08069cc0                .         .      8266         .         .         .
  ...
0x08069d68                .         .      1440         .         .         .
  ...
0x08069e40                .         .         .         .         .        64
  ...

Range: start = 0x089d1681, end = 0x0935ad00, increment = 00000004
Total =          0
  ...
Buffer allocation failed for the range 0x0935ad01-0x0972b3d0(00000004)
```

The following example shows collated output:

```
hostname# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<snip>
```

The following example shows the peak capture buffer:

```
hostname# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

The following example shows the peak capture buffer and the number of bytes that is held by the text/code that falls in the corresponding bucket address:

```
hostname# show memory profile peak detail
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

The following example shows the current state of memory profiling and the peak capture buffer:

```
hostname# show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a program text range of memory to profile.
clear memory profile	Clears the memory buffers held by the memory profiling function.

show memory tracking

To display currently allocated memory tracked by the tool, use the show memory tracking command in privileged EXEC mode.

show memory tracking [address | dump | detail]

Syntax Description

address	(Optional) Shows memory tracking by address.
detail	(Optional) Shows internal memory tracking state.
dump	(Optional) Dumps memory tracking address.

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(8)	This command was introduced.

Usage Guidelines

Use the **show memory tracking** command to show currently allocated memory tracked by the tool.

Examples

The following example shows the **show memory tracking** command out-put:

```
hostname# show memory tracking
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

The following examples show the **show memory tracking address**, and **show memory tracking dump** outputs:

```
hostname# show memory tracking address
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154

memory tracking by address:
```

```
37 byte region @ 0xa893ae80 allocated by 0x080c50f6
57 byte region @ 0xa893aed0 allocated by 0x080c5125
20481 byte region @ 0xa8d7cc50 allocated by 0x080c5154
17 byte region @ 0xa8a6f370 allocated by 0x080c50c2

hostname# memory tracking dump 0xa893aed0
Tracking data for the 57 byte region at 0xa893aed0:
Timestamp: 05:59:36.309 UTC Sun Jul 29 2007
Traceback:
0x080c5125
0x080b3695
0x0873f606
0x08740573
0x080ab530
0x080ac788
0x080ad141
0x0805df8f
Dumping 57 bytes of the 57 byte region:
a893aed0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893aee0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893aef0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893af00: 0c 0c 0c 0c 0c 0c 0c 0c 0c | .........
```

Related Commands

Command	Description
clear memory tracking	Clears all currently gathered information.
show memory tracking	Shows currently allocated memory.

show memory webvpn

To generate memory usage statistics for webvpn, use the **show memory webvpn** command in privileged EXEC mode.

show memory webvpn [allobjects | blocks | dumpstate [cache | disk0 | disk1 | flash | ftp | system | tftp]| pools | profile [clear | dump | start | stop] | usedobjects {{begin | exclude | grep | include} line *line***}]**

Syntax Description

allobjects	Displays webvpn memory consumption details for pools, blocks and all used and freed objects.
begin	Begins with the line that matches.
blocks	Displays webvpn memory consumption details for memory blocks.
cache	Specifies a filename for a webvpn memory cache state dump.
clear	Clears the webvpn memory profile.
disk0	Specifies a filename for webvpn memory disk0 state dump.
disk1	Specifies a filename for webvpn memory disk1 state dump:.
dump	Puts webvpn memory profile into a file.
dumpstate	Puts webvpn memory state into a file.
exclude	Excludes the line(s) that match.
flash	Specifies a filename for webvpn memory flash state dump.
ftp	Specifies a filename for webvpn memory ftp state dump.
grep	Includes/excludes lines that match.
include	Includes the line(s) that match.
line	Identifies the line(s) to match.
line	Specifies the line(s) to match.
pools	Show webvpn memory consumption details for memory pools.
profile	Gathers the webvpn memory profile and places it in a file.
system	Specifies a filename for webvpn memory system state dump.
start	Starts gathering the webvpn memory profile.
stop	Stops gathering the webvpn memory profile.
tftp	Specifies a filename for a webvpn memory tftp state dump.
usedobjects	Displays webvpn memory consumption details for used objects.

Defaults

No default behavior or value.

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	•	—	•	—	—
Global configuration	•	—	•	—	—
Webvpn mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following is sample output from the **show memory webvpn allobjects** command:

```
hostname# show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

Related Commands

Command	Description
memory-size	Sets the amount of memory on the adaptive security appliance that WebVPN services can use.

show memory-caller address

To display the address ranges configured on the adaptive security appliance, use the **show memory-caller address** command in privileged EXEC mode.

show memory-caller address

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

You must first configure an address ranges with the **memory caller-address** command before you can display them with the **show memory-caller address** command.

Examples

The following examples show the address ranges configured with the **memory caller-address** commands, and the resulting display of the **show memory-caller address** command:

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464

hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

If address ranges are not configured before entering the **show memory-caller address** command, no addresses display:

```
hostname# show memory-caller address
Move down stack frame for the addresses:
```

Related Commands

Command	Description
memory caller-address	Configures block of memory for the caller PC.

show mfib

To display MFIB in terms of forwarding entries and interfaces, use the **show mfib** command in user EXEC or privileged EXEC mode.

show mfib [*group* [*source*]] [**verbose**]

Syntax Description

group	(Optional) IP address of the multicast group.
source	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.
verbose	(Optional) Displays additional information about the entries.

Defaults

Without the optional arguments, information for all groups is shown.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

Related Commands

Command	Description
show mfib verbose	Displays detail information about the forwarding entries and interfaces.

show mfib active

To display active multicast sources, use the **show mfib active** command in user EXEC or privileged EXEC mode.

show mfib [*group*] **active** [*kbps*]

Syntax Description

group	(Optional) IP address of the multicast group.
kbps	(Optional) Limits the display to multicast streams that are greater-than or equal to this value.

This command has no arguments or keywords.

Defaults

The default value for *kbps* is 4. If a *group* is not specified, all groups are shown.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The output for the show mfib active command displays either positive or negative numbers for the rate PPS. The adaptive security appliance displays negative numbers when RPF packets fail or when the router observes RPF packets with an interfaces out (OIF) list. This type of activity may indicate a multicast routing problem.

Examples

The following is sample output from the **show mfib active** command:

```
hostname# show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)
```

```
Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

Related Commands

Command	Description
show mroute active	Displays active multicast streams.

show mfib count

To display MFIB route and packet count data, use the **show mfib count** command in user EXEC or privileged EXEC mode.

show mfib [*group* [*source*]] **count**

Syntax Description

group	(Optional) IP address of the multicast group.
source	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.

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 or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command displays packet drop statistics.

Examples

The following sample output from the **show mfib count** command:

```
hostname# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

Related Commands

Command	Description
clear mfib counters	Clears MFIB router packet counters.
show mroute count	Displays multicast route counters.

show mfib interface

To display packet statistics for interfaces that are related to the MFIB process, use the **show mfib interface** command in user EXEC or privileged EXEC mode.

show mfib interface [*interface*]

Syntax Description

interface	(Optional) Interface name. Limits the display to the specified interface.

Defaults

Information for all MFIB interfaces is shown.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.

show mfib reserved

To display reserved groups, use the **show mfib reserved** command in user EXEC or privileged EXEC mode.

show mfib reserved [**count** | **verbose** | **active** [*kpbs*]]

Syntax Description

count	(Optional) Displays packet and route count data.
verbose	(Optional) Displays additional information.
active	(Optional) Displays active multicast sources.
kpbs	(Optional) Limits the display to active multicast sources greater-than or equal to this value.

Defaults

The default value for *kbps* is 4.

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 or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command displays MFIB entries in the range 224.0.0.0 through 224.0.0.225.

Examples

The following is sample output from the **show mfib reserved** command:

```
hostname# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per
second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface
Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
```

```
dmz Flags: IC
inside Flags: IC
```

Related Commands

Command	Description
show mfib active	Displays active multicast streams.

show mfib status

To display the general MFIB configuration and operational status, use the **show mfib status** command in user EXEC or privileged EXEC mode.

show mfib status

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 or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show mfib status** command:

```
hostname# show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.

show mfib summary

To display summary information about the number of MFIB entries and interfaces, use the **show mfib summary** command in user EXEC or privileged EXEC mode.

show mfib summary

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show mfib summary** command:

```
hostname# show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

Related Commands

Command	Description
show mroute summary	Displays multicast routing table summary information.

show mfib verbose

To display detail information about the forwarding entries and interfaces, use the **show mfib verbose** command in user EXEC or privileged EXEC mode.

show mfib verbose

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 or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show mfib verbose** command:

```
hostname# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.
show mfib summary	Displays summary information about the number of MFIB entries and interfaces.

show mgcp

To display MGCP configuration and session information, use the **show mgcp** command in privileged EXEC mode.

show mgcp {**commands** | **sessions**} [**detail**]

Syntax Description

commands	Lists the number of MGCP commands in the command queue.
sessions	Lists the number of existing MGCP sessions.
detail	(Optional) Lists additional information about each command (or session) in the output.

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
Preexisting	This command was preexisting.

Usage Guidelines

The **show mgcp commands** command lists the number of MGCP commands in the command queue. The **show mgcp sessions** command lists the number of existing MGCP sessions. The **detail** option includes additional information about each command (or session) in the output.

Examples

The following are examples of the **show mgcp** command options:

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
hostname#

hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP | host-pc-2
        Transaction ID  2052
        Endpoint name | aaln/1
        Call ID | 9876543210abcdef
```

```
        Connection ID |
        Media IP | 192.168.5.7
        Media port | 6058
hostname#

hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
hostname#

hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
        Gateway IP | host-pc-2
        Call ID | 9876543210abcdef
        Connection ID | 6789af54c9
        Endpoint name | aaln/1
        Media lcl port  6166
        Media rmt IP | 192.168.5.7
        Media rmt port  6058
hostname#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug mgcp	Enables MGCP debug information.
inspect mgcp	Enables MGCP application inspection.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show conn	Displays the connection state for different connection types.

show mmp

To display information about existing MMP sessions, use the **show mmp** command in privileged EXEC mode.

show mmp [*address*]

Syntax Description

address	Specifies the IP address of an MMP client/server.

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(4)	The command was introduced.

Examples

The following example shows the use of the **show mmp** command to display information about existing MMP sessions:

```
hostname# show mmp 10.0.0.42
MMP session:: inside:10.0.0.42/5443 outside:172.23.62.204/2442
session-id=71AD3EB1-7BE8-42E0-8DC3-E96E41D4ADD5
data:: rx-bytes=1258, tx-bytes=1258
```

Related Commands

Command	Description
debug mmp	Displays inspect MMP events.
inspect mmp	Configures the MMP inspection engine.
show debug mmp	Displays current debug settings for the MMP inspection module.

show mode

To show the security context mode for the running software image and for any image in Flash memory, use the **show mode** command in privileged EXEC mode.

show mode

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 mode** command. The following example shows the current mode and the mode for the non-running image “image.bin”:

```
hostname# show mode flash:/image.bin
Firewall mode: multiple
```

The mode can be multiple or single.

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
mode	Sets the context mode to single or multiple.

show module

To show information about the SSM installed on the ASA 5500 series adaptive security appliance, information about the SSC installed on the ASA 5505 adaptive security appliance, information about the SSP installed on the ASA 5585-X adaptive security appliances, information about the IPS SSP installed on an ASA 5585-X adaptive security appliance, and system information, use the **show module** command in user EXEC mode.

show module [**all** | *slot* [**details** | **recover**]]

Syntax Description

all	(Default) Shows information for the SSM in slot 1 and the device in slot 0.
details	(Optional) Shows additional information, including remote management configuration for intelligent SSMs (for example, ASA-SSM-*x*0).
recover	(Optional) For intelligent SSMs, shows the settings for the **hw-module module recover** command. **Note** The **recover** keyword is valid only when you have created a recovery configuration for the SSM by using the **configure** keyword with the **hw-module module recover** command.
slot	(Optional) Specifies the slot number, 0 or 1. Slot 0 is the adaptive security appliance base device.

Defaults

The information appears for both slots.

Command Modes

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

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

1. The **show module recover** command is only available in the system execution space.

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	More detail was added to the output.
8.2(1)	Information about the SSC has been added to the output.
8.2(5)	Information about the ASA 5585-X adaptive security appliances and the IPS SSP installed on an ASA 5585-X adaptive security appliance has been added to the output.

Usage Guidelines

This command shows information about the SSC, SSM, SSP, and device and built-in interfaces.

Examples

The following is sample output from the **show module** command. Slot 0 is the base device; slot 1 is a CSC SSM.

```
hostname> show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c30d to 000b.fcf8.c311  1.0          1.0(10)0     7.1(0)5
  1 000b.fcf8.012c to 000b.fcf8.012c  1.0          1.0(10)0     CSC SSM 5.0 (Build#1187)

Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
  1 CSC SSM scan services are not
  1 CSC SSM                        5.0 (Build#1187)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

Table 22 describes each field listed in the output.

Table 3 show module Output Fields

Field	Description
Mod	The slot number, 0 or 1.
Card Type	For the device shown in slot 0, the type is the platform model. For the SSM in slot 1, the type is the SSM type.
Model	The model for this slot.
Serial No.	The serial number.
MAC Address Range	The MAC address range for interfaces on this SSM or, for the device, the built-in interfaces.
Hw Version	The hardware version.
Fw Version	The firmware version.
Sw Version	The software version.
SSM Application Name	The name of the application running on the SSM.
SSM Application Version	The version of the application running on the SSM.

Table 3 show module Output Fields (continued)

Field	Description
Status	For the device in slot 0, the status is Up Sys. The status of the SSM in slot 1 can be any of the following: • Initializing—The SSM is being detected and the control communication is being initialized by the device. • Up—The SSM has completed initialization by the device. • Unresponsive—The device encountered an error while communicating with this SSM. • Reloading—For intelligent SSMs, the SSM is reloading. • Shutting Down—The SSM is shutting down. • Down—The SSM is shut down. • Recover—For intelligent SSMs, the SSM is attempting to download a recovery image.
Data Plane Status	The current state of the data plane.
Compatibility	The compatibility of the SSM relative to the rest of the device.

The output of the **show module details** command varies according to which SSM or SSP is in the slot. For example, output for the CSC SSM includes fields about components of the CSC SSM software. These fields do not appear if the slot has an AIP SSM instead. The following is generic sample output from the **show module details** command:

```
hostname> show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   V1.0
Serial Number:      12345678
Firmware version:   1.0(7)2
Software version:   4.1(1.1)S47(0.1)
MAC Address Range:  000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       10.89.147.13
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

Table 23 describes each field listed in the output.

Table 4 show module details Output Fields

Field	Description
Mgmt IP addr	For intelligent SSMs, shows the IP address for the SSM management interface.
Mgmt web ports	For intelligent SSMs, shows the ports configured for the management interface.
Mgmt TLS enabled	For intelligent SSMs, shows whether transport layer security is enabled (true or false) for connections to the management interface of the SSM.

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

```
hostname> show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask:           255.255.255.0
Gateway IP Address:  10.1.2.254
```

The following is sample output from the **show module 1 details** command when an SSC is installed:

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5505 Security Services Card
Model: ASA-SSC
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App. Name: IPS
App. Status: Up
App. Status Desc:
App. Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
                  209.165.202.158/32
                  209.165.200.254/24
Mgmt Vlan: 20
```

The following is sample output from the **show module 1 details** command when an IPS SSP is installed in an ASA 5585-X adaptive security appliance:

```
hostname# show module 1 details
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------------------
  0 ASA 5585 Secruity Services Processor w 8GE,2 ASA5585-SSP        JAF1417BDNP
  1 ASA 5585 Security Services Processor w 8GE,2 ASA5585-SSP-IPS10  JAF1417BDQM

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 5475.d029.7b70 to 5475.d029.7b7b  1.0          0.0(0)0      8.2(3)
  1 5475.d029.7bc4 to 5475.d029.7bcf  1.0          0.0(0)0

Mod SSM Application Name           Status          SSM Application Version
--- ------------------------------ ----------------------------------------

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up Sys             Not Applicable
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the SSM booting process.
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the intelligent SSM software.
hw-module module shutdown	Closes the SSM software in preparation for being powered off without losing configuration data.

show monitor-interface

To display information about the interfaces monitored for failover, use the **show monitor-interface** command in privileged EXEC mode.

show monitor-interface

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.
8.2(2)	This command was modified. The output includes IPv6 addresses.

Usage Guidelines

Because an interface can have more than one IPv6 address configured on it, only the link-local address is displayed in the **show monitor-interface** command. If both IPv4 and IPv6 addresses are configured on an interface, both addresses appear in the output. If there is no IPv4 address configured on the interface, the IPv4 address in the output appears as 0.0.0.0. If there is no IPv6 address configured on an interface, the address is simply omitted from the output.

Monitored failover interfaces can have the following status:

- Unknown—Initial status. This status can also mean the status cannot be determined.
- Normal—The interface is receiving traffic.
- 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.
- Testing—Hello messages are not heard on the interface for five poll times.
- Link Down—The interface or VLAN is administratively down.
- No Link—The physical link for the interface is down.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

Examples

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

```
hostname# show monitor-interface

This host: Primary - Active
                Interface outside (10.86.94.88): Normal (Waiting)
                Interface management (192.168.1.1): Normal (Waiting)
                Interface failif (0.0.0.0/fe80::223:4ff:fe77:fed): Normal (Waiting)
        Other host: Secondary - Failed
                Interface outside (0.0.0.0): Unknown (Waiting)
                Interface management (0.0.0.0): Unknown (Waiting)
                Interface failif (0.0.0.0): Unknown (Waiting)
```

Related Commands

Command	Description
monitor-interface	Enables health monitoring on a specific interface

show mrib client

To display information about the MRIB client connections, use the **show mrib client** command in user EXEC or privileged EXEC mode.

show mrib client [**filter**] [**name** *client_name*]

Syntax Description

filter	(Optional) Displays client filter. Used to view information about the MRIB flags that each client owns and the flags in which each clients is interested.
name *client_name*	(Optional) Name of a multicast routing protocol that acts as a client of MRIB, such as PIM or IGMP.

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 or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **filter** option is used to display the route and interface level flag changes that various MRIB clients have registered. This command option also shows what flags are owned by the MRIB clients.

Examples

The following sample output from the **show mrib client** command using the **filter** keyword:

```
hostname# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
```

```
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

Related Commands

Command	Description
show mrib route	Displays MRIB table entries.

show mrib route

To display entries in the MRIB table, use the **show mrib route** command in user EXEC or privileged EXEC mode.

show mrib route [[*source* | *****] [*group*[*/prefix-length*]]]

Syntax Description

*	(Optional) Display shared tree entries.
/prefix-length	(Optional) Prefix length of the MRIB route. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
group	(Optional) IP address or name of the group.
source	(Optional) IP address or name of the route source.

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 or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The MFIB table maintains a subset of entries and flags updated from MRIB. The flags determine the forwarding and signaling behavior according to a set of forwarding rules for multicast packets.

In addition to the list of interfaces and flags, each route entry shows various counters. Byte count is the number of total bytes forwarded. Packet count is the number of packets received for this entry. The **show mfib count** command displays global counters independent of the routes.

Examples

The following is sample output from the **show mrib route** command:

```
hostname# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
```

```
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

Related Commands

Command	Description
show mfib count	Displays route and packet count data for the MFIB table.
show mrib route summary	Displays a summary of the MRIB table entries.

show mroute

To display the IPv4 multicast routing table, use the **show mroute** command in privileged EXEC mode.

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

Syntax Description

active *rate*	(Optional) Displays only active multicast sources. Active sources are those sending at the specified *rate* or higher. If the *rate* is not specified, active sources are those sending at a rate of 4 kbps or higher.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
group	(Optional) IP address or name of the multicast group as defined in the DNS hosts table.
pruned	(Optional) Displays pruned routes.
reserved	(Optional) Displays reserved groups.
source	(Optional) Source hostname or IP address.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the multicast routing table.

Defaults

If not specified, the *rate* argument defaults to 4 kbps.

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 mroute** command displays the contents of the multicast routing table. The adaptive security appliance populates the multicast routing table by creating (S,G) and (*,G) entries based on PIM protocol messages, IGMP reports, and traffic. The asterisk (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (through RPF).

To view the **mroute** commands in the running configuration, use the **show running-config mroute** command.

Examples

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

```
hostname(config)# show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

The following fields are shown in the **show mroute** output:

- **Flags**—Provides information about the entry.
  - **D—Dense**. Entry is operating in dense mode.
  - **S—Sparse**. Entry is operating in sparse mode.
  - **B—Bidir Group**. Indicates that a multicast group is operating in bidirectional mode.
  - **s—SSM Group**. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.
  - **C—Connected**. A member of the multicast group is present on the directly connected interface.
  - **L—Local**. The adaptive security appliance itself is a member of the multicast group. Groups are joined locally by the **igmp join-group** command (for the configured group).
  - **I—Received Source Specific Host Report**. Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by IGMP. This flag is set only on the DR.
  - **P—Pruned**. Route has been pruned. The software keeps this information so that a downstream member can join the source.
  - **R—RP-bit set**. Indicates that the (S, G) entry is pointing toward the RP.
  - **F—Register flag**. Indicates that the software is registering for a multicast source.
  - **T—SPT-bit set**. Indicates that packets have been received on the shortest path source tree.
  - **J—Join SPT**. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the adaptive security appliance to join the source tree.

For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the adaptive security appliance monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute.

Note The adaptive security appliance measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.

If the default SPT-Threshold value of 0 kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the adaptive security appliance immediately switches to the shortest path source tree when traffic from a new source is received.

- **Timers:Uptime/Expires**—Uptime indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. Expires indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.
- **Interface state**—Indicates the state of the incoming or outgoing interface.
  - **Interface**—The interface name listed in the incoming or outgoing interface list.
  - **State**—Indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists or a time-to-live (TTL) threshold.
- **(*, 239.1.1.40)** and **(* , 239.2.2.1)**—Entries in the IP multicast routing table. The entry consists of the IP address of the source followed by the IP address of the multicast group. An asterisk (*) in place of the source indicates all sources.
- **RP**—Address of the RP. For routers and access servers operating in sparse mode, this address is always 224.0.0.0.
- **Incoming interface**—Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
- **RPF nbr**—IP address of the upstream router to the source.
- **Outgoing interface list**—Interfaces through which packets will be forwarded.

Related Commands

Command	Description
clear configure mroute	Removes the **mroute** commands from the running configuration.
mroute	Configures a static multicast route.
show mroute	Displays IPv4 multicast routing table.
show running-config mroute	Displays configured multicast routes.

show nac-policy

To show the NAC policy usage statistics and the assignment of NAC policies to group policies, use the **show nac-policy** command in privileged EXEC mode.

show nac-policy [*nac-policy-name*]

Syntax Description

nac-policy-name	(Optional) Name of the NAC policy for which to display usage statistics.

Defaults

If you do not specify a name, the CLI lists all NAC policy names along with their respective statistics.

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.

Examples

The following example shows the data for the NAC policies named framework1 and framework2:

```
asa2(config)# show nac-policy
nac-policy framework1 nac-framework
  applied session count = 0
  applied group-policy count = 2
  group-policy list:    GroupPolicy2    GroupPolicy1
nac-policy framework2 nac-framework is not in use.
```

The first line of each NAC policy indicates its name and type (nac-framework). The CLI shows the text "is not in use" next to the policy type if the policy is not assigned to any group policies. Otherwise, the CLI displays the usage data for the group policy. Table 26-5 explains the fields in the **show nac-policy** command.

Table 26-5 show nac-policy Command Fields

Field	Description
applied session count	Cumulative number of VPN sessions to which this adaptive security appliance applied the NAC policy.

Table 26-5 show nac-policy Command Fields

Field	Description
applied group-policy count	Cumulative number of group polices to which this adaptive security appliance applied the NAC policy.
group-policy list	List of group policies to which this NAC policy is assigned. In this case, the usage of a group policy does not determine whether it appears in this list; if the NAC policy is assigned to a group policy in the running configuration, then the group policy appears in this list.

Related Commands

clear nac-policy	Resets the NAC policy usage statistics.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
show vpn-session_summary.db	Displays the number IPSec, Cisco WebVPN, and NAC sessions.

show nameif

To view the interface name set using the **nameif** command, use the show nameif command in privileged EXEC mode.

show nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

Syntax Description

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.

Defaults

If you do not specify an interface, the adaptive security appliance shows all interface names.

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
Preexisting	This command was preexisting.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name in a context. The output for this command shows only the mapped name in the Interface column.

Examples

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

```
hostname# show nameif
Interface               Name                    Security
GigabitEthernet0/0      outside                 0
GigabitEthernet0/1      inside                  100
GigabitEthernet0/2      test2                   50
```

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 ip brief	Shows the interface IP address and status.

show nat

To display NAT policy counters, use the **show nat** command in privileged EXEC mode.

show nat *src_ifc* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

Syntax Description

dst_ifc	(Optional) Specifies destination interface to filter.
dst_ip	(Optional) Specifies destination IP address to filter.
dst_mask	(Optional) Specifies mask for destination IP address.
src_ifc	(Optional) Specifies source interface to filter.
src_ip	(Optional) Specifies source IP address to filter.
src_mask	(Optional) Specifies mask for source IP address.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

When a **static**, **nat**, or **alias** command is configured, it is internally converted into NAT policies between applicable interfaces. The **show nat** command displays the policies that are looked up when translations or untranslations are performed.

The NAT policy output consists of the following information:

- The match clause for the traffic that should be matched
- The action to be taken after a match, which could be any of the following
  - static translation
  - alias translation
  - identity NAT
  - NAT exempt
  - implicit deny because no translation group wa s found
- counters—translate_hits provide counters for real to mapped address conversion and untranslate_hits provide counters for mapped to real address conversion.

Examples

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

```
hostname(config)# show nat

NAT policies on Interface inside:
  match ip inside host 192.168.200.101 outside any
    static translation to 128.106.254.8
    translate_hits = 0, untranslate_hits = 0

NAT policies on Interface management:
  match ip management any outside 1.1.1.0 255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any inside 1.1.1.0 255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any test 1.1.1.0 255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any management 1.1.1.0 255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any outside any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
  match ip management any inside any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
  match ip management any test any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
  match ip management any management any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
```

Related Commands

Command	Description
clear nat counters	Clears NAT policy counters.
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
nat-control	Enables/disables NAT configuration requirement.
nat-rewrite	Enables NAT rewrite for IP addresses embedded in the A-record of a DNS response.

show ntp associations

To view NTP association information, use the **show ntp associations** command in user EXEC mode.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Shows additional details about each association.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

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

Examples

The following is sample output from the **show ntp associations** command:

```
hostname> show ntp associations
     address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 26-6 shows each field description.

Table 26-6 show ntp associations Fields

Field	Description
(leading characters in display lines)	The first characters in a display line can be one or more of the following characters: • * —Synchronized to this peer. • # —Almost synchronized to this peer. • + —Peer selected for possible synchronization. • - —Peer is a candidate for selection. • ~ —Peer is statically configured, but not synchronized.
address	The address of the NTP peer.
ref clock	The address of the reference clock of the peer.
st	The stratum of the peer.
when	The time since the last NTP packet was received from the peer.
poll	The polling interval (in seconds).
reach	The peer reachability (as a bit string, in octal).
delay	The round-trip delay to the peer (in milliseconds).
offset	The relative time of the peer clock to the local clock (in milliseconds).
disp	The dispersion value.

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

```
hostname> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87   0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74   0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62   16000.0
```

Table 26-7 shows each field description.

Table 26-7 show ntp associations detail Fields

Field	Description
IP-address configured	The server (peer) IP address.
(status)	• our_master—The adaptive security appliance is synchronized to this peer. • selected—Peer is selected for possible synchronization. • candidate—Peer is a candidate for selection.
(sanity)	• sane—The peer passes basic sanity checks. • insane—The peer fails basic sanity checks.
(validity)	• valid—The peer time is believed to be valid. • invalid—The peer time is believed to be invalid. • leap_add—The peer is signalling that a leap second will be added. • leap-sub—The peer is signalling that a leap second will be subtracted.
stratum	The stratum of the peer.
(reference peer)	unsynced—The peer is not synchronized to any other machine. ref ID—The address of the machine that the peer is synchronized to.
time	The last time stamp the peer received from its master.
our mode client	Our mode relative to the peer, which is always client.
peer mode server	The peer's mode relative to us, which is always server.
our poll intvl	Our poll interval to the peer.
peer poll intvl	The peer poll interval to us.
root delay	The delay along the path to the root (ultimate stratum 1 time source).
root disp	The dispersion of the path to the root.
reach	The peer reachability (as a bit string in octal).
sync dist	The peer synchronization distance.
delay	The round-trip delay to the peer.
offset	The offset of the peer clock relative to our clock.
dispersion	The dispersion of the peer clock.
precision	The precision of the peer clock (in hertz).
version	The NTP version number that the peer is using.
org time	The originate time stamp.
rcv time	The receive time stamp.
xmt time	The transmit time stamp.
filtdelay	The round-trip delay (in milliseconds) of each sample.
filtoffset	The clock offset (in milliseconds) of each sample.
filterror	The approximate error of each sample.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the adaptive security appliance to use in packets for authentication with an NTP server.
show ntp status	Shows the status of the NTP association.

show ntp status

To show the status of each NTP association, use the **show ntp status** command in user EXEC mode.

show ntp status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

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

Examples

The following is sample output from the **show ntp status** command:

```
hostname> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

Table 26-8 shows each field description.

Table 26-8 show ntp status Fields

Field	Description
Clock	• synchronized—The adaptive security appliance is synchronized to an NTP server. • unsynchronized—The adaptive security appliance is not synchronized to an NTP server.
stratum	NTP stratum of this system.

Table 26-8 show ntp status Fields

Field	Description
reference	The address of the NTP server to which the adaptive security appliance is synchronized.
nominal freq	The nominal frequency of the system hardware clock.
actual freq	The measured frequency of the system hardware clock.
precision	The precision of the clock of this system (in hertz).
reference time	The reference time stamp.
clock offset	The offset of the system clock to the synchronized peer.
root delay	The total delay along the path to the root clock.
root dispersion	The dispersion of the root path.
peer dispersion	The dispersion of the synchronized peer.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the adaptive security appliance to use in packets for authentication with an NTP server.
show ntp associations	Shows the NTP servers with which the adaptive security appliance is associated.

show ospf

To display the general information about the OSPF routing processes, use the **show ospf** command in privileged EXEC mode.

show ospf [*pid* **[***area_id***]**]

Syntax Description

area_id	(Optional) ID of the area that is associated with the OSPF address range.
pid	(Optional) The ID of the OSPF process.

Defaults

Lists all OSPF processes if no *pid* is specified.

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
Preexisting	This command was preexisting.

Usage Guidelines

If the *pid* is included, only information for the specified routing process is included.

Examples

The following is sample output from the **show ospf** command, showing how to display general information about a specific OSPF routing process:

```
hostname# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

The following is sample output from the **show ospf** command, showing how to display general information about all OSPF routing processes:

```
hostname# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
```

```
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf border-routers

To display the internal OSPF routing table entries to ABRs and ASBRs, use the **show ospf border-routers** command in privileged EXEC mode.

show ospf border-routers

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
Preexisting	This command was preexisting.

Examples

The following is sample output from the show **ospf border-routers** command:

```
hostname# show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf database

To display the information contained in the OSPF topological database on the adaptive security appliance, use the **show ospf database** command in privileged EXEC mode.

show ospf [*pid* [*area_id*]] **database** [**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**] [*lsid*] [**internal**] [**self-originat**e | **adv-router** *addr*]

show ospf [*pid* [*area_id*]] **database database-summary**

Syntax Description

addr	(Optional) Router address.
adv-router	(Optional) Advertised router.
area_id	(Optional) ID of the area that is associated with the OSPF address range.
asbr-summary	(Optional) Displays an ASBR list summary.
database	Displays the database information.
database-summary	(Optional) Displays the complete database summary list.
external	(Optional) Displays routes external to a specified autonomous system.
internal	(Optional) Routes that are internal to a specified autonomous system.
lsid	(Optional) LSA ID.
network	(Optional) Displays the OSPF database information about the network.
nssa-external	(Optional) Displays the external not-so-stubby-area list.
pid	(Optional) ID of the OSPF process.
router	(Optional) Displays the router.
self-originate	(Optional) Displays the information for the specified autonomous system.
summary	(Optional) Displays a summary of the list.

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
Preexisting	This command was preexisting.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the adaptive security appliance. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

Examples

The following is sample output from the **show ospf database** command:

```
hostname# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

The following is sample output from the **show ospf database asbr-summary** command:

```
hostname# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

The following is sample output from the **show ospf database router** command:

```
hostname# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
```

```
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

The following is sample output from the **show ospf database network** command:

```
hostname# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

The following is sample output from the **show ospf database summary** command:

```
hostname# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

The following is sample output from the **show ospf database external** command:

```
hostname# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf flood-list

To display a list of OSPF LSAs waiting to be flooded over an interface, use the **show ospf flood-list** command in privileged EXEC mode.

show ospf flood-list *interface_name*

Syntax Description

interface_name	The name of the interface for which to display neighbor 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
Preexisting	This command was preexisting.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the adaptive security appliance. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

Examples

The following is sample output from the **show ospf flood-list** command:

```
hostname# show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf interface

To display the OSPF-related interface information, use the **show ospf interface** command in privileged EXEC mode.

show ospf interface [*interface_name*]

Syntax Description

interface_name	(Optional) Name of the interface for which to display the OSPF-related 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
Preexisting	This command was preexisting.

Usage Guidelines

When used without the *interface_name* argument, the OSPF information for all interfaces is shown.

Examples

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

```
hostname# show ospf interface inside
inside is up, line protocol is up
Internet Address 192.168.254.202, Mask 255.255.255.0, Area 0.0.0.0
AS 201, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 192.168.254.10, Interface address 192.168.254.10
Backup Designated router id 192.168.254.28, Interface addr 192.168.254.28
Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
Hello due in 0:00:05
Neighbor Count is 8, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.254.28 (Backup Designated Router)
  Adjacent with neighbor 192.168.254.10 (Designated Router)
```

Related Commands

Command	Description
interface	Opens interface configuration mode.

show ospf neighbor

To display the OSPF-neighbor information on a per-interface basis, use the **show ospf neighbor** command in privileged EXEC mode.

show ospf neighbor [**detail** | *interface_name* [*nbr_router_id*]]

Syntax Description

detail	(Optional) Lists detail information for the specified router.
interface_name	(Optional) Name of the interface for which to display neighbor information.
nbr_router_id	(Optional) Router ID of the neighbor router.

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
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show ospf neighbor** command. It shows how to display the OSPF-neighbor information on a per-interface basis.

```
hostname# show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

Command	Description
neighbor	Configures OSPF routers interconnecting to non-broadcast networks.
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf request-list

To display a list of all LSAs that are requested by a router, use the **show ospf request-list** command in privileged EXEC mode.

show ospf request-list *nbr_router_id interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information. Displays the list of all LSAs that are requested by the router from this interface.
nbr_router_id	Router ID of the neighbor router. Displays the list of all LSAs that are requested by the router from this neighbor.

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
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show ospf request-list** command:

```
hostname# show ospf request-list 192.168.1.12 inside

          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

Related Commands

Command	Description
show ospf retransmission-list	Displays a list of all LSAs waiting to be resent.

show ospf retransmission-list

To display a list of all LSAs waiting to be resent, use the **show ospf retransmission-list** command in privileged EXEC mode.

show ospf retransmission-list *nbr_router_id interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information.
nbr_router_id	Router ID of the neighbor router.

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
Preexisting	This command was preexisting.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the adaptive security appliance. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

The *nbr_router_id* argument displays the list of all LSAs that are waiting to be resent for this neighbor.

The *interface_name* argument displays the list of all LSAs that are waiting to be resent for this interface.

Examples

The following is sample output from the **show ospf retransmission-list** command, where the *nbr_router_id* argument is 192.168.1.11 and the *if_name* argument is outside:

```
hostname# show ospf retransmission-list 192.168.1.11 outside

          OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2


  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

Related Commands

Command	Description
show ospf request-list	Displays a list of all LSAs that are requested by a router.

show ospf summary-address

To display a list of all summary address redistribution information that is configured under an OSPF process, use the **show ospf summary-address** command in privileged EXEC mode.

show ospf summary-address

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
Preexisting	This command was preexisting.

Examples

The following shows sample output from the **show ospf summary-address** command. It shows how to display a list of all summary address redistribution information before a summary address has been configured for an OSPF process with the ID of 5.

```
hostname# show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

Related Commands

Command	Description
summary-address	Creates aggregate addresses for OSPF.

show ospf virtual-links

To display the parameters and the current state of OSPF virtual links, use the **show ospf virtual-links** command in privileged EXEC mode.

show ospf virtual-links

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
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show ospf virtual-links** command:

```
hostname# show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

show perfmon

To display information about the performance of the adaptive security appliance, use the **show perfmon** command in privileged EXEC mode.

show perfmon [**detail**]

Syntax Description

detail	(Optional) Shows additional statsistics. These statistics match those gathered by the Global and Per-protocol connection objects of the Cisco Unified Firewall MIB.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Support for this command was introduced on the adaptive security appliance.
7.2(1)	The **detail** keyword was added.

Usage Guidelines

This command output does not display in a Telnet session.

The **perfmon** command shows performance statistics continuously at defined intervals. The **show perfmon** command allows you to display the information immediately.

Examples

The following is sample output for the **show perfmon** command:

```
hostname(config)# show perfmon
Context: my_context
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
TCP Intercept        0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
```

```
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

The following is sample output for the **show perfmon detail** command:

```
hostname(config)# show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept        0/s          0/s

SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

Related Commands

Command	Description
perfmon	Displays detailed performance monitoring information at defined intervals.

show phone-proxy

To show phone-proxy specific information, use the **show phone-proxy** command in global configuration mode.

show phone-proxy [media-sessions [detail] | signaling-sessions [detai] | secure-phones]

Syntax Description

detail	Displays detailed information.
media-sessions	Displays the corresponding media sessions stored by the Phone Proxy. In addition, displays the media-termination address configured for the interface between which the media sessions are established.
secure-phones	Displays the phones capable of secure mode stored in the database.
signaling-sessions	Displays the corresponding signaling sessions stored by the Phone Proxy.

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	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.
8.2(1)	The command was updated so that specifying the **media-sessions** keyword also displays the media-termination address configured for the interface between which the media sessions are established.

Examples

The following example shows the use of the **show phone proxy** command to show Phone Proxy specific information:

```
hostname(config)# show phone-proxy
Phone-Proxy 'mypp': Runtime Proxy ref_cnt 2
Cluster Mode: nonsecure
Run-time proxies:
Proxy 0xd55f6fd8: Class-map: secsip, Inspect: sip
Proxy 0xd58a93a8: Class-map: secsccp, Inspect: skinny
phoneproxy(config)# show phone-proxy secure-phones
mypp: 5 in use, 5 most used
Interface  IP Address     Port  MAC            Timeout Idle
outside    69.181.112.219 10889 001e.7ac4.da9c 0:05:00 0:01:36
outside    98.208.25.87   14159 001c.581c.0663 0:05:00 0:00:04
outside    98.208.25.87   14158 0007.0e36.4804 0:05:00 0:00:13
outside    98.208.25.87   14157 001e.7ac4.deb8 0:05:00 0:00:21
```

```
outside    128.107.254.69 49875 001b.0cad.1f69 0:05:00 0:00:04
hostname(config)#
```

The following example shows the use of the **show phone proxy** command to display the phones capable of secure mode stored in the database:

```
hostname(config)# show phone-proxy secure-phones
asa_phone_proxy: 3 in use, 4 most used

Interface/IP Address      MAC               Timeout    Idle
------------------------  ----------        ---------  ------
outside:69.181.112.219    001e.7ac4.da9c    0:05:00    0:00:16
outside:69.181.112.219    0002.b9eb.0aad    0:05:00    0:00:58
outside:98.208.49.30      0007.0e36.4804    0:05:00    0:00:09
hostname(config)#
```

The following example shows the use of the show phone proxy command to Show output from a successful call and the media-termination address configured for the interface between which the media sessions are established:

```
hostname(config)# show phone-proxy media-sessions
Media-session: 128.106.254.3/1168 refcnt 6
  <---> RTP connection to 192.168.200.106/25038 tx_pkts 485 rx_pkts 491
Media-session: 128.106.254.3/1170 refcnt 6
  <---> SRTP connection to 98.208.25.87/1030 tx_pkts 484 rx_pkts 485
```

Related Commands

Command	Description
debug phone-proxy	Displays debug messages for the Phone Proxy instance.
phone proxy	Configures the Phone Proxy instance.

show pim df

To display the bidirectional DF "winner" for a rendezvous point (RP) or interface, use the **show pim df** command in user EXEC or privileged EXEC mode.

show pim df [**winner**] [*rp_address* | *if_name*]

Syntax Description

rp_address	Can be either one of the following: • Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4 host** command. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.
if_name	The physical or logical interface name.
winner	(Optional) Displays the DF election winner per interface per RP.

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 or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command also displays the winner metric towards the RP.

Examples

The following is sample output from the **show pim df** command:

```
hostname# show df winner inside
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

To display group-to-protocol mapping table, use the **show pim group-map** command in user EXEC or privileged EXEC mode.

show pim group-map [**info-source**] [*group*]

Syntax Description

group	(Optional) Can be either one of the following: • Name of the multicast group, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
info-source	(Optional) Displays the group range information source.

Defaults

Displays group-to-protocol mappings for all groups.

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 or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command displays all group protocol address mappings for the RP. Mappings are learned on the adaptive security appliance from different clients.

The PIM implementation on the adaptive security appliance has various special entries in the mapping table. Auto-rp group ranges are specifically denied from sparse-mode group range. SSM group range also does not fall under sparse-mode. Link Local multicast groups (224.0.0.0–224.0.0.225, as defined by 224.0.0.0/24) are also denied from the sparse-mode group range. The last entry shows all remaining groups in Sparse-Mode with a given RP.

If multiple RPs are configured with the **pim rp-address** command, then the appropriate group range is displayed with their corresponding RPs.

Examples

The following is sample output form the **show pim group-map** command:

```
hostname# show pim group-map
Group Range      Proto   Client Groups   RP address   Info
```

```
224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

In lines 1 and 2, Auto-RP group ranges are specifically denied from the sparse mode group range.

In line 3, link-local multicast groups (224.0.0.0 to 224.0.0.255 as defined by 224.0.0.0/24) are also denied from the sparse mode group range.

In line 4, the PIM Source Specific Multicast (PIM-SSM) group range is mapped to 232.0.0.0/8.

The last entry shows that all the remaining groups are in sparse mode mapped to RP 10.10.3.2.

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the adaptive security appliance.
pim rp-address	Configures the address of a PIM rendezvous point (RP).

show pim interface

To display interface-specific information for PIM, use the **show pim interface** command in user EXEC or privileged EXEC mode.

show pim interface [*if_name* | **state-off** | **state-on**]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
state-off	(Optional) Displays interfaces with PIM disabled.
state-on	(Optional) Displays interfaces with PIM enabled.

Defaults

If you do not specify an interface, PIM information for all interfaces is shown.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The PIM implementation on the adaptive security appliance considers the adaptive security appliance itself a PIM neighbor. Therefore, the neighbor count column in the output of this command shows one more than the actual number of neighbors.

Examples

The following example displays PIM information for the inside interface:

```
hostname# show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR     DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1      172.16.1.4
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the adaptive security appliance.

show pim join-prune statistic

To display PIM join/prune aggregation statistics, use the **show pim join-prune statistics** command in user EXEC or privileged EXEC mode.

show pim join-prune statistics [*if_name*]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

Defaults

If an interface is not specified, this command shows the join/prune 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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Clear the PIM join/prune statistics with the **clear pim counters** command.

Examples

The following is sample output from the **show pim join-prune statistic** command:

```
hostname# show pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received

            inside   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
         Ethernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet3   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet2   0 /    0 /    0         0 /    0 /    0
```

Related Commands

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim neighbor

To display entries in the PIM neighbor table, use the **show pim neighbor** command in user EXEC or privileged EXEc mode.

show pim neighbor [**count** | **detail**] [*interface*]

Syntax Description

interface	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
count	(Optional) Displays the total number of PIM neighbors and the number of PIM neighbors on each interface.
detail	(Optional) Displays additional address of the neighbor learned through the upstream-detection hello option.

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 or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is used to determine the PIM neighbors known to this router through PIM hello messages. Also, this command indicates that an interface is a designated router (DR) and when the neighbor is capable of bidirectional operation.

The PIM implementation on the adaptive security appliance considers the adaptive security appliance itself to be a PIM neighbor. Therefore, the adaptive security appliance interface is shown in the output of this command. The IP address of the adaptive security appliance is indicated by an asterisk next to the address.

Examples

The following is sample output from the **show pim neighbor** command:

```
hostname# show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the adaptive security appliance.

show pim range-list

To display range-list information for PIM, use the **show pim range-list** command in user EXEC or privileged EXEC mode.

show pim range-list [*rp_address*]

Syntax Description

rp_address	Can be either one of the following: • Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4 host** command. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.

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 or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is used to determine the multicast forwarding mode to group mapping. The output also indicates the rendezvous point (RP) address for the range, if applicable.

Examples

The following is sample output from the **show pim range-list** command:

```
hostname# show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

Related Commands

Command	Description
show pim group-map	Displays group-to-PIM mode mapping and active RP information.

show pim topology

To display PIM topology table information, use the **show pim topology** command in user EXEC or privileged EXEC mode.

show pim topology [*group*] [*source*]

Syntax Description

group	(Optional) Can be one of the following: • Name of the multicast group, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
source	(Optional) Can be one of the following: • Name of the multicast source, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast source. This is a multicast IP address in four-part dotted-decimal notation.

Defaults

Topology information for all groups and sources is shown.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the MRIB, which is an intermediary for communication between multicast routing protocols, such as PIM, local membership protocols, such as Internet Group Management Protocol (IGMP), and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

Note For forwarding information, use the **show mfib route** command.

Examples

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

```
hostname# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

Related Commands

Command	Description
show mrib route	Displays the MRIB table.
show pim topology reserved	Displays PIM topology table information for reserved groups.

show pim topology reserved

To display PIM topology table information for reserved groups, use the **show pim topology reserved** command in user EXEC or privileged EXEC mode.

show pim topology reserved

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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# show pim topology reserved

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside            00:02:26  off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside             00:00:48  off II
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show pim topology route-count

To display PIM topology table entry counts, use the **show pim topology route-count** command in user EXEC or privileged EXEC mode.

show pim topology route-count [**detail**]

Syntax Description

detail	(Optional) Displays more detailed count information on a per-group basis.

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**
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command displays the count of entries in the PIM topology table. To display more information about the entries, use the **show pim topology** command.

Examples

The following is sample output from the **show pim topology route-count** command:

```
hostname# show pim topology route-count

PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show pim traffic

To display PIM traffic counters, use the **show pim traffic** command in user EXEC or privileged EXEC mode.

show pim 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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Clear the PIM traffic counters with the **clear pim counters** command.

Examples

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

```
hostname# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                      0        9485
Hello                                  0        9485
Join-Prune                             0           0
Register                               0           0
Register Stop                          0           0
Assert                                 0           0
Bidir DF Election                      0           0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Send Errors                                        0
Packet Sent on Loopback Errors                     0
Packets Received on PIM-disabled Interface         0
Packets Received with Unknown PIM Version          0
```

Related Commands

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim tunnel

To display information about the PIM tunnel interfaces, use the **show pim tunnel** command in user EXEC or privileged EXEC mode.

show pim tunnel [*if_name*]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

Defaults

If an interface is not specified, this command shows the PIM tunnel information 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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

PIM register packets are sent through the virtual encapsulation tunnel interface from the source first hop DR router to the RP. On the RP, a virtual decapsulation tunnel is used to represent the receiving interface of the PIM register packets. This command displays tunnel information for both types of interfaces.

Register tunnels are the encapsulated (in PIM register messages) multicast packets from a source that is sent to the RP for distribution through the shared tree. Registering applies only to SM, not SSM and bidirectional PIM.

Examples

The following is sample output from the **show pim tunnel** command:

```
hostname# show pim tunnel

Interface     RP Address Source Address

Encapstunnel0 10.1.1.1   10.1.1.1
Decapstunnel0 10.1.1.1   -
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show power inline

For models with PoE interfaces, such as the ASA 5505 adaptive security appliance, use the **show power inline** command in user EXEC mode to show power status of the interfaces.

show power inline

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
7.2(1)	This command was introduced.

Usage Guidelines

You can use PoE interfaces to connect devices that require power, such as an IP phone or a wireless access point.

Examples

The following is sample output from the **show power inline** command:

```
hostname> show power inline

  Interface     Power   Device
  -----------   -----   ------
  Ethernet0/0    n/a    n/a
  Ethernet0/1    n/a    n/a
  Ethernet0/2    n/a    n/a
  Ethernet0/3    n/a    n/a
  Ethernet0/4    n/a    n/a
  Ethernet0/5    n/a    n/a
  Ethernet0/6    On     Cisco
  Ethernet0/7    Off    n/a
```

Table 26-9 shows each field description:

Table 26-9 show power inline Fields

Field	Description
Interface	Shows all interfaces on the adaptive security appliance, including ones that do not have PoE available.
Power	Shows whether the power is On or Off. If a device does not need power, if there is no device on that interface, or if the interface is shut down the value is Off. If the interface does not support PoE, then the value is n/a.
Device	Shows the type of device obtaining power, either Cisco or IEEE. If the device does not draw power, the value is n/a. The display shows Cisco when the device is a Cisco powered device. IEEE indicates that the device is an IEEE 802.3af- compliant powered device.

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
clear interface	Clears counters for the **show interface** command.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show priority-queue statistics

To display the priority queue statistics for an interface, use the **show priority-queue statistics** command in privileged EXEC mode.

show priority-queue statistics [*interface-name*]

Syntax Description

interface-name	(Optional) Specifies the name of the interface for which you want to show the best-effort and low-latency queue details.

Defaults

If you omit the interface name, this command shows priority queue statistics for all configured interfaces. For 10-Gigabit Ethernet interfaces on the ASA 5585-X adaptive security appliance only, the statistics are aggregate statistics for all 10-Gigabit Ethernet interfaces, and this command displays the same statistics for all 10-Gigabit Ethernet 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.
8.2(3)	The output was modified to show uplink statistics for all 10-Gigabit Ethernet interfaces on the ASA 5585-X adaptive security appliances only.

Examples

The following example shows the use of the **show priority-queue statistics** command for non 10-Gigabit Ethernet interfaces for the interface named test. In this output, BE indicates the best-effort queue, and LLQ represents the low-latency queue:

Note Uplink statistics are displayed in the output only for 10-Gigabit Ethernet interfaces on the ASA 5585-X adaptive security appliances. Uplink statistics do not appear in the output for 1-Gigabit Ethernet interfaces on the ASA 5585-X adaptive security appliances.

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test
(Uplink statistics is displayed for all TenGigabitEthernet interfaces)

Queue Type      = BE
Tail Drops        = 0
Reset Drops       = 0
```

```
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
(Uplink statistics is displayed for all TenGigabitEthernet interfaces)

Queue Type      = LLQ
Tail Drops        = 0
Reset Drops       = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
```

Related Commands

Command	Description
clear configure priority-queue	Removes the priority queue configuration from the named interface.
clear priority-queue statistics	Clears the priority queue statistics counters for an interface or for all configured interfaces.
priority-queue	Configures priority queueing on an interface.
show running-config priority-queue	Shows the current priority queue configuration on the named interface.

show processes

To display a list of the processes that are running on the adaptive security appliance, use the **show processes** command in privileged EXEC mode.

show processes [cpu-usage | *non-zero* **|** *sorted***] [cpu-hog | memory | internals]**

Syntax Description

non-zero	(Optional) Shows processes with non-zero CPU usage.
sorted	(Optional) Shows sorted CPU usage for processes

Defaults

By default this command displays the processes running on the adaptive security appliance.

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)	Support for this command was introduced.
7.0(4)	The Runtime value was enhanced to display accurracy within one millisecond.
7.2(1)	The output display was enhanced to display more detailed information about processes that hog the CPU.
8.0(1)	Added the **show process cpu-usage** argument.

Usage Guidelines

The **show processes** command allows you to display a list of the processes that are running on the adaptive security appliance.

The command can also help determine what process is using the CPU, with the optional **cpu-usage or cpu-hog** arguments. A process is flagged if it is hogging the CPU for more than 100 milliseconds.

The **show process cpu-usage** command displays the processes running on the adaptive security appliance and the CPU usage statistics for the last 5 seconds, 1 minute and 5 minutes. The adaptive security appliance administrators can use this command to narrow down a particular process on the adaptive security appliance that might be utilizing the CPU of the adaptive security appliance. The additional arguments *sorted* and *non-zero* can be used to further customize the output of the command.

The **show process cpu-hog** command displays the following columns when invoked:

- MAXHOG - Maximum CPU hog runtime in milliseconds.
- NUMHOG - Number of CPU hog runs.
- LASTHOG - Last CPU hog runtime in milliseconds.

- PC - Instruction pointer of the CPU hogging process
- Traceback - Stack trace of the CPU hogging process

Processes are lightweight threads requiring only a few instructions. In the listing, PC is the program counter, SP is the stack pointer, STATE is the address of a thread queue, Runtime is the number of milliseconds that the thread has been running based on CPU clock cycles, SBASE is the stack base address, Stack is the current number of bytes that are used and the total size of the stack, and Process lists the thread's function.

The runtime value displays accurracy within one millisecond for complete and accurate accounting of process CPU usage based on CPU clock cycles (<10ns resolution) instead of clock ticks (10ms resolution).

The traceback can have up to 14 addresses.

With the scheduler and total summary lines, you can run two consecutive **show proccess** commands and compare the output to determine:

- Where 100% of the CPU time was spent.
- What % of CPU is used by each thread, by comparing a thread's runtime delta to the total runtime delta.

The optional **memory** argument displays the memory allocated by each process, to help track memory usage by process.

The optional **internals** argument displays the number of invoked calls and giveups. Invoked is the number of times the scheduler has invoked, or ran, the process. Giveups is the number of times the process yielded the CPU back to the scheduler.

Examples

This example shows how to display a list of processes that are running on the adaptive security appliance:

```
hostname(config)# show processes

    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->

-     -        -         -        638515    -         -     scheduler
-     -        -         -       2625389    -         -     total
```

```
hostname(config)# show proc cpu-usage non-zero
PC         Thread      5Sec    1Min    5Min    Process
0818af8e   d482f92c    0.1%    0.1%    0.1%    Dispatch Unit
08bae136   d48180f0    0.1%    0.0%    0.2%    ssh
-------------------------------------

hostname(config)# show processes cpu

Process: ci/console, NUMHOG: 1, MAXHOG: 210, LASTHOG: 210 LASTHOG At:  01:08:24 UTC Jul 24
2005
PC:          153412
Traceback:    1532de  15352a  14b66d  14ba61 148c30 14930e  1125d1

Process: fover_parse, NUMHOG: 2, MAXHOG: 200, LASTHOG: 200
LASTHOG At:   02:08:24 UTC Jul 24 2005
PC:           6ff434
Traceback:    6ff838  6fe3a7  6fe424  6fe5ab 7060b7 3bfa44  1125d1

hostname(config)# show processes memory

------------------------------------------------------------
Allocs   Allocated       Frees         Freed         Process
          (bytes)                      (bytes)
------------------------------------------------------------
23512    13471545        6             180           *System Main*
0        0               0             0             lu_rx
2        8324            16            19488         vpnlb_thread
(other lines deleted for brevity)


hostname# show processes internals

     Invoked      Giveups  Process
           1            0  block_diag
    19108445     19108445  Dispatch Unit
           1            0  CF OIR
           1            0  Reload Control Thread
           1            0  aaa
           2            0  CMGR Server Process
           1            0  CMGR Timer Process
           2            0  dbgtrace
          69            0  557mcfix
    19108019     19108018  557poll
           2            0  557statspoll
           1            0  Chunk Manager
         135            0  PIX Garbage Collector
           6            0  route_process
           1            0  IP Address Assign
           1            0  QoS Support Module
           1            0  Client Update Task
        8973         8968  Checkheaps
           6            0  Session Manager
```

```
                237          235  uauth
(other lines deleted for brevity)
```

show reload

To display the reload status on the adaptive security appliance, use the **show reload** command in privileged EXEC mode.

show reload

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	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

The following example shows that a reload is scheduled for 12:00 a.m. (midnight) on Saturday, April 20:

```
hostname# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

Related Commands

Command	Description
reload	Reboots and reloads the configuration.

show resource allocation

To show the resource allocation for each resource across all classes and class members, use the **show resource allocation** command in privileged EXEC mode.

show resource allocation [**detail**]

Syntax Description

detail	Shows additional 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
7.2(1)	This command was introduced.

Usage Guidelines

This command shows the resource allocation, but does not show the actual resources being used. See the **show resource usage** command for more information about actual resource usage.

Examples

The following is sample output from the **show resource allocation** command. The display shows the total allocation of each resource as an absolute value and as a percentage of the available system resources.

```
hostname# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]                35000           N/A
 Inspects [rate]             35000           N/A
 Syslogs [rate]              10500           N/A
 Conns                      305000           30.50%
 Hosts                       78842           N/A
 SSH                            35           35.00%
 Telnet                         35           35.00%
 Xlates                      91749           N/A
 All                       unlimited
```

Table 26-10 shows each field description.

Table 26-10 show resource allocation Fields

Field	Description
Resource	The name of the resource that you can limit.
Total	The total amount of the resource that is allocated across all contexts. The amount is an absolute number of concurrent instances or instances per second. If you specified a percentage in the class definition, the adaptive security appliance converts the percentage to an absolute number for this display.
% of Avail	The percentage of the total system resources that is allocated across all contexts, if available. If a resource does not have a system limit, this column shows N/A.

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

```
hostname# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Telnet           default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Xlates           default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      23040      23040     N/A
                 bronze             0      CA      11520
                 All Contexts:      3                         23040     N/A

mac-addresses    default          all       C      65535
                 gold               1       D      65535      65535    100.00%
                 silver             1      CA       6553       6553      9.99%
                 bronze             0      CA       3276
                 All Contexts:      3                        137623    209.99%
```

Table 26-11 shows each field description.

Table 26-11 show resource allocation detail Fields

Field	Description
Resource	The name of the resource that you can limit.
Class	The name of each class, including the default class. The All contexts field shows the total values across all classes.
Mmbrs	The number of contexts assigned to each class.
Origin	The origin of the resource limit, as follows: • A—You set this limit with the **all** option, instead of as an individual resource. • C—This limit is derived from the member class. • D—This limit was not defined in the member class, but was derived from the default class. For a context assigned to the default class, the value will be "C" instead of "D." The adaptive security appliance can combine "A" with "C" or "D."
Limit	The limit of the resource per context, as an absolute number. If you specified a percentage in the class definition, the adaptive security appliance converts the percentage to an absolute number for this display.
Total	The total amount of the resource that is allocated across all contexts in the class. The amount is an absolute number of concurrent instances or instances per second. If the resource is unlimited, this display is blank.
% of Avail	The percentage of the total system resources that is allocated across all contexts in the class, if available. If the resource is unlimited, this display is blank. If the resource does not have a system limit, this column shows N/A.

Related Commands

Command	Description
class	Creates a resource class.
context	Adds a security context.
limit-resource	Sets the resource limit for a class.
show resource types	Shows the resource types for which you can set limits.
show resource usage	Shows the resource usage of the adaptive security appliance.

show resource types

To view the resource types for which the adaptive security appliance tracks usage, use the **show resource types** command in privileged EXEC mode.

show resource types

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.
7.2(1)	This command shows additional resource types that you can manage for each context.

Examples

The following sample display shows the resource types:

```
hostname# show resource types

Rate limited resource types:
  Conns           Connections/sec
  Inspects        Inspects/sec
  Syslogs         Syslogs/sec

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  Mac-addresses   MAC Address table entries
  ASDM            ASDM Connections
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  All             All Resources
```

Related Commands

Command	Description
clear resource usage	Clears the resource usage statistics
context	Adds a security context.
show resource usage	Shows the resource usage of the adaptive security appliance.

show resource usage

To view the resource usage of the adaptive security appliance or for each context in multiple mode, use the **show resource usage** command in privileged EXEC mode.

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system** | **detail**] [**resource** {[**rate**] *resource_name* | **all**}] [**counter** *counter_name* [*count_threshold*]]

Syntax Description

context *context_name*	(Multiple mode only) Specifies the context name for which you want to view statistics. Specify **all** for all contexts; the adaptive security appliance lists the context usage for each context.
count_threshold	Sets the number above which resources are shown. The default is 1. If the usage of the resource is below the number you set, then the resource is not shown. If you specify **all** for the counter name, then the *count_threshold* applies to the current usage. **Note** To show all resources, set the *count_threshold* to **0**.
counter *counter_name*	Shows counts for the following counter types: • **current**—Shows the active concurrent instances or the current rate of the resource. • **peak**—Shows the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted. • **denied**—Shows the number of instances that were denied because they exceeded the resource limit shown in the Limit column. • **all**—(Default) Shows all statistics.
detail	Shows the resource usage of all resources, including those you cannot manage. For example, you can view the number of TCP intercepts.

resource [**rate**] *resource_name*	Shows the usage of a specific resource. Specify **all** (the default) for all resources. Specify **rate** to show the rate of usage of a resource. Resources that are measured by rate include **conns**, **inspects**, and **syslogs**. You must specify the **rate** keyword with these resource types. The conns resource is also measured as concurrent connections; only use the **rate** keyword to view the connections per second. Resources include the following types: • **asdm**—ASDM management sessions. • **conns**—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • **inspects**—Application inspections. • **hosts**—Hosts that can connect through the adaptive security appliance. • **mac-addresses**—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. • **ssh**—SSH sessions. • **syslogs**—System log messages. • **telnet**—Telnet sessions. • **xlates**—NAT translations.
summary	(Multiple mode only) Shows all context usage combined.
system	(Multiple mode only) Shows all context usage combined, but shows the system limits for resources instead of the combined context limits.
top *n*	(Multiple mode only) Shows the contexts that are the top *n* users of the specified resource. You must specify a single resource type, and not **resource all**, with this option.

Defaults

For multiple context mode, the default context is **all**, which shows resource usage for every context. For single mode, the context name is ignored and the output shows the "context" as "System."

The default resource name is **all**, which shows all resource types.

The default counter name is **all**, which shows all statistics.

The default count threshold is **1**.

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.
7.2(1)	This command now shows the denied resources, because you can now limit the resources for each context.

Examples

The following is sample output from the **show resource usage context** command, which shows the resource usage for the admin context:

```
hostname# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

The following is sample output from the **show resource usage summary** command, which shows the resource usage for all contexts and all resources. This sample shows the limits for 6 contexts.

```
hostname# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
Conns [rate]              270          535      42200       1704 Summary
Inspects [rate]           270          535     100000(S)       0 Summary
U = Some contexts are unlimited and are not included in the total.
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

The following is sample output from the **show resource usage system** command, which shows the resource usage for all contexts, but it shows the system limit instead of the combined context limits:

```
hostname# show resource usage system

Resource              Current         Peak      Limit    Denied  Context
Telnet                      3            5        100         0  System
SSH                         5            7        100         0  System
Conns                      40           55        N/A         0  System
Hosts                      44           56        N/A         0  System
```

The following is sample output from the **show resource usage detail counter all 0** command, which shows all resources, and not just those you can manage:

```
hostname# show resource usage detail counter all 0

Resource              Current         Peak      Limit        Denied Context
memory                1012028      1538428  unlimited             0 admin
chunk:aaa                   0            0  unlimited             0 admin
chunk:aaa_queue             0            0  unlimited             0 admin
chunk:acct                  0            0  unlimited             0 admin
chunk:channels             25           39  unlimited             0 admin
chunk:CIFS                  0            0  unlimited             0 admin
chunk:conn                  0            0  unlimited             0 admin
chunk:crypto-conn           0            0  unlimited             0 admin
chunk:dbgtrace              1            2  unlimited             0 admin
chunk:dhcpd-radix           0            0  unlimited             0 admin
chunk:dhcp-relay-r          0            0  unlimited             0 admin
chunk:dhcp-lease-s          0            0  unlimited             0 admin
chunk:dnat                  0            0  unlimited             0 admin
```

```
chunk:ether                 0           0  unlimited           0 admin
chunk:est                   0           0  unlimited           0 admin

...

Telnet                      0           0          5           0 admin
SSH                         1           1          5           0 admin
ASDM                        0           1          5           0 admin
Syslogs [rate]              0          68  unlimited           0 admin
aaa rate                    0           0  unlimited           0 admin
url filter rate             0           0  unlimited           0 admin
Conns                       1           6  unlimited           0 admin
Xlates                      0           0  unlimited           0 admin
tcp conns                   0           0  unlimited           0 admin
Hosts                       2           3  unlimited           0 admin
udp conns                   0           0  unlimited           0 admin
smtp-fixups                 0           0  unlimited           0 admin
Conns [rate]                0           7  unlimited           0 admin
establisheds                0           0  unlimited           0 admin
pps                         0           0  unlimited           0 admin
syslog rate                 0           0  unlimited           0 admin
bps                         0           0  unlimited           0 admin
Fixups [rate]               0           0  unlimited           0 admin
non tcp/udp conns           0           0  unlimited           0 admin
tcp-intercepts              0           0  unlimited           0 admin
globals                     0           0  unlimited           0 admin
np-statics                  0           0  unlimited           0 admin
statics                     0           0  unlimited           0 admin
nats                        0           0  unlimited           0 admin
ace-rules                   0           0        N/A           0 admin
aaa-user-aces               0           0        N/A           0 admin
filter-rules                0           0        N/A           0 admin
est-rules                   0           0        N/A           0 admin
aaa-rules                   0           0        N/A           0 admin
console-access-rul          0           0        N/A           0 admin
policy-nat-rules            0           0        N/A           0 admin
fixup-rules                 0           0        N/A           0 admin
aaa-uxlates                 0           0  unlimited           0 admin
CP-Traffic:IP               0           0  unlimited           0 admin
CP-Traffic:ARP              0           0  unlimited           0 admin
CP-Traffic:Fixup            0           0  unlimited           0 admin
CP-Traffic:NPCP             0           0  unlimited           0 admin
CP-Traffic:Unknown          0           0  unlimited           0 admin
```

Related Commands

Command	Description
class	Creates a resource class.
clear resource usage	Clears the resource usage statistics
context	Adds a security context.
limit-resource	Sets the resource limit for a class.
show resource types	Shows a list of resource types.

show rip database

To display the information contained in the RIP topological database, use the **show rip database** command in privileged EXEC mode.

show rip database [*ip_addr* [*mask*]]

Syntax Description

ip_addr	(Optional) Limits the display routes for the specified network address.
mask	(Optional) Specifies the network mask for the optional network address.

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
7.2(1)	This command was introduced.

Usage Guidelines

The RIP routing-related **show** commands are available in privileged mode on the adaptive security appliance. You do not need to be in an RIP configuration mode to use the RIP-related **show** commands.

The RIP database contains all of the routes learned through RIP. Routes that appear in this database may not necessarily appear in the routing table. Refer to the *Cisco Security Appliance Command Line Configuration Guide* for information about how the routing table is populated from the routing protocol databases.

Examples

The following is sample output from the **show rip database** command:

```
hostname# show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

The following is sample output from the **show rip database** command with a network address and mask:

```
Router# show rip database 172.19.86.0 255.255.255.0
```

```
172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

Related Commands

Command	Description
router rip	Enables RIP routing and configures global RIP routing parameters.

show route

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

show route [*interface_name* [*ip_address* [*netmask* [**static**]]]]

Syntax Description

static	(Optional) Limits the display to static routes.
interface_name	(Optional) Limits the display to route entries that use the specified interface.
ip_address	(Optional) Limits the display to routes to the specified destination.
netmask	(Optional) Network mask to apply to *ip_address*.

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
Preexisting	This command was preexisting.

Usage Guidelines

The **show route** command lists the "best" routes for new connections. When you send a permitted TCP SYN to the backup interface, the adaptive security appliance can only respond using the same interface. If there is no default route in the RIB on that interface, the adaptive security appliance drops the packet because of no adjacency. Everything that is configured as shown in the **show running-config route** command is maintained in certain data structures in the system.

You can check the backend interface-specific routing table with the **show asp table routing** command. This design is similar to OSPF or EIGRP, in which the protocol-specific route database is not the same as the global routing table, which only displays the "best" routes. This behavior is by design.

Examples

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

```
hostname# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

The following is sample output of the show route command on the ASA5505 adaptive adaptive security appliance. It displays the internal loopback address, which is used by the VPN Hardware Client for individual user authentication.

```
hostname(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

Note When using the **show ip route** command in Cisco IOS, the **longer-prefix** keyword is available. Using this keyword in Cisco IOS, the route is only displayed when the specified network and mask pair match. On ASA, the longer-prefix keyword is the default behaviour for the **show rout**e command; that is, no additonal keyword is needed in the CLI. Because of this, you cannot see the route when you type **ip**. To get the super-net route, the mask value needs to be passed along with the IP address.

Related Commands

Command	Description
clear configure route	Removes the **route** commands from the configuration that do not contain the **connect** keyword.
route	Creates a static or default route.
show running-config route	Displays the route commands in the running configuration.