CHAPTER 27

show isakmp sa through show route Commands

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
1.1(1)	This command was introduced.

Usage Guidelines

The output from this command includes the following fields:

Detail not specified.

Table 27-1

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

Table 27-2

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
hostname(config)# sho 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 FWSM.
show running-config isakmp	Displays all the active ISAKMP configuration.

show isakmp stats

To display runtime statistics, use the **show isakmp stats** command in 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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.

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the FWSM.
show running-config isakmp	Displays all the active ISAKMP configuration.

show local-host

To display the IP addresses of hosts that initiated current connections through the FWSM, use the **show local-host** command in privileged EXEC mode. This command also shows the address translation, if present, and the number of TCP, UDP, and embryonic connections per host.

show local-host [*ip_address*] [**detail**] [**all**]

Syntax Description

all	(Optional) Shows all initiating hosts, including connections to or from the FWSM. If you do not use the **all** keyword, connections to the FWSM and from the FWSM do not display.
detail	(Optional) Displays detailed network states.
ip_address	(Optional) Specifies the initiating 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
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.
2.3(1)	Because the TCP intercept feature was changed to use SYN cookies, this command no longer shows embryonic connections above the embryonic connection limit.

Usage Guidelines

In most cases, the "local host" is the initiating host. However, if you configure static NAT for an IP address, that host always shows as the local host even if they did not initiate the connection.

If you configure outside NAT (either static NAT or NAT exemption), and an inside host initiates a connection to the outside host, both the inside and outside hosts are listed as local hosts in the **show local-host** output. This feature lets you track connection limits for both hosts.

If you configure an embryonic connection limit, and the limit is exceeded, the FWSM implements TCP intercept to prevent a SYN attack. After TCP intercept is triggered, additional embryonic connections do not appear in the **show local-host** output.

The connection limits are set using the **nat** or **static** commands, or using the **set connection** commands.

Examples

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

```
hostname# show local-host
local host: <10.5.59.30>, tcp conn(s)/limit = 1/0, embryonic(s)/limit =
0/0 udp conn(s)/limit = 0/0
    Xlate(s):
        Global 10.5.59.30 Local 10.5.59.30
```

Table 27-3 show local-host Fields

Field	Description
local host: <*ip_address*>	Shows the host IP address.
tcp conn(s)/limit = *x*/*y*	Shows the current TCP connections followed by the connection limit. 0 means no limit was set.
embryonic(s)/limit = *x*/*y*	Shows the current embryonic connections followed by the connection limit. 0 means no limit was set.
udp conn(s)/limit = *x*/*y*	Shows the current UDP connections followed by the connection limit. 0 means no limit was set.
Xlate(s):	Shows the address translation. The FWSM shows the same address for local and global if you did not configure NAT, or if you configured identity NAT or NAT exemption.

Related Commands

Command	Description
clear local-host	Clears connections.
nat	Associates a network with a pool of global IP addresses.
show conns	Shows connection information.
static	Statically translates an address.
set connection	Sets connection limits.

show logging

To show syslogs currently in the log buffer or to show other logging settings, use the **show logging** command in privileged EXEC mode.

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

Syntax Description

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

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
Preexisting	This command was preexisting.

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 lets 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

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 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 message	Sets the message level, or disables messages.
logging queue	Configures the logging queue.

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
2.2(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
3.1	This command was introduced.

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 FWSM.
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**]

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
2.2(1)	This command was introduced.

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.

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

Examples

The following 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: 15958088 bytes (24%)
Used memory:
Allocated memory in use: 29680332 bytes (44%)
Reserved memory: 21470444 bytes (32%)
----------------------------- ----------------
```

```
Total memory: 67108864 bytes (100%)

Least free memory: 4551716 bytes ( 7%)
Most used memory: 62557148 bytes (93%)

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

fragment size count total
(bytes) (bytes)
---------------- ---------- --------------
16 8 128
24 4 96
32 2 64
40 5 200
64 3 192
88 1 88
168 1 168
224 1 224
256 1 256
296 2 592
392 1 392
400 1 400
1816 1 1816*
4435968 1 4435968**
11517504 1 11517504

* - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

fragment size count total
(bytes) (bytes)
---------------- ---------- --------------
40 50 2000
48 144 6912
56 24957 1397592
64 101 6464
72 99 7128
80 1032 82560
88 18 1584
96 64 6144
104 57 5928
112 6 672
120 112 13440
128 15 1920
136 87 11832
144 22 3168
152 31 4712
160 90 14400
168 65 10920
176 74 13024
184 11 2024
192 8 1536
200 1 200
<output omitted>
```

Related Commands

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

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
3.1(1)	Support for 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 FWSM.
show memory profile	Displays information about the memory usage (profiling) of the FWSM.
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:

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

Command History

Release	Modification
3.1(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 27-4 describes the significant fields in the **show memory delayed-free-poisoner** command output.

Table 27-4 **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 FWSM, 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
3.1(1)	Support for 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 FWSM might experience a temporary reduction in performance when memory profiling is enabled

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 (below) 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 = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
<snip>
```

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 held:

```
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).

Command	Description
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-caller address

To display the address ranges configured on the FWSM, 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
3.1(1)	Support for 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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 FWSM 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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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]
           Vlan101     up    [        no,       no]
           Vlan102     up    [        no,       no]
           Vlan103     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 privileged EXEC mode.

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

Syntax Description

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

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**
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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
2.2(1)	This command was introduced.

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

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
```

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 mode

To show the security context mode, 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
2.2(1)	This command was introduced.

Examples

The following is sample output from the **show mode** command.

```
hostname# show mode
Firewall mode: multiple
The flash mode is the SAME as the running mode.
```

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 mrib client

To display information about the MRIB client connections, use the **show mrib client** command in 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 mrib route summary

To display a summary of the MRIB table entries, use the **show mrib route summary** command in privileged EXEC mode.

show mrib route 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

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

```
hostname# show mrib route summary
MRIB Route-DB Summary
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 0
```

Related Commands

Command	Description
show mrib route	Displays 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
3.1(1)	This command was introduced.

Usage Guidelines

The **show mroute** command displays the contents of the multicast routing table. The FWSM 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 FWSM 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 FWSM 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 FWSM 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 FWSM 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 FWSM 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 nameif

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

show nameif [*mapped_name*]

Syntax Description

mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.

Defaults

If you do not specify an interface, the FWSM 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
1.1(1)	This command was introduced.

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
Vlan20 outside                0
Vlan35 inside                 100
Vlan36 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 np

To display information about the network processors, use the **show np** command in privileged EXEC mode.

show np {*number item* | **all**}

Syntax Description

show np	Shows the maximum and free s in each side (ingress or egress) in each NP and the amount of time thresholds were reached in each NP.
number	The network processor number, in single digit format. You can enter **1**, **2**, or **3**.

item	Use the following values to display information about the corresponding item: **aaa**—Show slow-path aaa information **acl**—Show slow-path acl information **alias**—Show slow-path alias information ***arp***—Show arp information **buffer**—Show slow-path buffer information **cab**—Show cab information **cs**—Show control store information **egress** —Show egress **epc**—Show EPC statistics **established**—Show slow-path established information ***asr-table***—Show asr-table information **flow-control**—Show flow control information **global**—Show slow-path global information **fogrp-table**—Show fogrp-table information **global-table**—Show global-table information **hw-status**—Show hw-status **interface-vlan**—Show interface-vlan information **mac**—Show mac information **mcast**—Show mcast information **mroute**—Show slow-path mroute information **nat**—Show slow-path nat information **pif**—Show interface information **reassembly**—Show slow-path reassembly information **route**—Show route information **semaphore**—Show semaphore information **shun**—Show slow-path shun information **smtp**—Show slow-path smtp information **static**—Show slow-path static information **stats**—Show fp statistics **status**—Show status **thread**—Show thread information **uauth** Show—slow-path uauth information **syn-cookie**—Show syn-cookie **vft**—Show vft table information **vlan**—Show vlan information.
all	Displays all NP 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
3.1	This is command was introduced.

Usage Guidelines

The **show np** command displays the amount of time thresholds were reached in each NP.

Examples

The following is sample output from the **show np** command in single mode:

```
hostname# show np
               MAX   FREE   THRESH_0   THRESH_1   THRESH_2
NP1 (ingress)  32768  32768          0          0          0
    (egress)  521206 521206          0          0          0
NP2 (ingress)  32768  32768          0          0          0
    (egress)  521206 521206          0          0          0
NP3 (ingress)  32768  32768          0          0          0
    (egress)  521206 521206          0          0          0
hostname(config-ctx)#
```

The following is sample output from the **show np asr-table** command in single mode:

```
hostname# show np 1 asr-table all
--------------------------------------------------------------------------------
                              ASR Table (NP-1)
--------------------------------------------------------------------------------
ASR Group |    Vlan Entries in ASR Group (0 denotes empty slot)
--------------------------------------------------------------------------------
        1 |       0      0      0      0      0      0      0      0
...
       32 |       0      0      0      0      0      0      0      0
--------------------------------------------------------------------------------
hostname#
```

The following is sample output from the **show np 1 flow-control** command in single mode:

```
hostname# show np 1 flow-control
Flow control for np 1
   REGISTER             ADDRESS      DATA
   i_tx_prob            0x30000000   0x7f7f7f7f
   i_rand_num           0x30000100   0x33994fbb
   i_fq_th              0xa0400020   0x00000000
   e_tx_prob            0xb0000000   0x7f7f7f7f
   e_rand_num           0xb0001000   0x7f7f7f7f
   p0_twin_th           0xa0400100   0x0007ffff
   p1_twin_th           0xa0400200   0x0007ffff
```

```
   e_p0_ewma_th          0xa0400400   0x0007ffff
   e_p1_ewma_th          0xa0400800   0x0007ffff
   ewma_k                0xa0400040   0x00000000
   ewma_t                0xa0400080   0x00000000
   res_data_cfg          0xa0000880   0x00000003
```

The following is sample output from the **show np 1 fogrp-table all** command in single mode:

```
hostname# show np 1 fogrp-table all
--------------------------------------------------------------------------------
                         Failover Group Table (NP-1)
--------------------------------------------------------------------------------
Failover Group ID                    : 0
My MAC address                       : 0005.9a38.8100
Other MAC address                    : 0000.0000.0000
Flags                                : 0x1
   |- Failover Stop Traffic          : 0
   |- Logical Update Enabled         : 0
   |- Logical Update Sync HTTP       : 0
   |- Logical Update Force Sync      : 0
   `- Failover Active                : 1
--------------------------------------------------------------------------------
```

The following is sample output from the **show np 1 global-table** command in single mode:

```
hostname# sh np 1 global-table
...
--------------------------------------------------------------------------------
                             Global Table (NP-1)
--------------------------------------------------------------------------------
Admin VCID                           : 1
Global Flags                         : 0x2000
   |- Virtual Mode                   : 0
   |- Failover                       : 0
   |- Failover State                 : 1
   |- Logical Update                 : 0
   |- LU_Sync_HTTP                   : 0
   |- Fixup ICMP                     : 0
   `- Fixup ICMP Error               : 0
LU Interface                         : 0
LU Time                              : 15000
DestMAC Address of LU interface      : 0x000000000000
SrcMAC Address of LU interface       : 0x000000000000
Vlan ID in LU packet                 : 0
Type for LU packets                  : 0xaaaa
Originating blade                    : 0
--------------------------------------------------------------------------------
hostname#
```

The following is sample output from the **show np 1 hw-status** command in single mode:

```
hostname# sh np 1 hw-status

Hw status for np 1
   REGISTER              ADDRESS      DATA
   my_tb                 0xa0004080   0x00000000
   local_tb              0xa0004100   0x80000000
   local_mc_tb           0xa0004200   0x80000000
   init_done             0xa0008200   0xffff8000
   ready                 0xa0040020   0x80000000
   pll_lock              0xa0000220   0x00000000
   bcb_fq_th_0           0xa0001010   0x03000000
   bcb_fq_th_1           0xa0001020   0x05000000
   bcb_fq_th_2           0xa0001040   0x0a000000
```

```
   bcb_fq_th_GT         0xa0001080   0x40000000
   ppc_boot_redir       0x38000117   0x00000000
   ppc_watchdog         0xa0004800   0x00000000
   thread_enable        0xa0008020   0xffffffff
   gfh_data             0x24c00030   0x00000000
   i_max_dispatch       0x24400c40   0x80000000
   e_max_dispatch       0x24400c50   0x80000000
   semaphore            0x25000180   0x00000000
   tp_ds_map            0xa0000140   0xaaaaaaaa
   e_sdm_stack_th       0xa0001800   0x80000000
   fq_es_max            0xa0002100   0x00000000
   fq_es_th_0           0xa0002010   0x06000000
   fq_es_th_1           0xa0002020   0x08000000
   fq_es_th_2           0xa0002040   0x20000000
   discard_qcb          0xa0001400   0x00000029
   bw_alloc             0xa0002800   0x00000000
   fcb_fq_size          0xa0002200   0x40000000
   dmu_cfg_A            0xa0010010   0x00000000
   dmu_cfg_B            0xa0010020   0x00000000
   dmu_cfg_C            0xa0010040   0x00000000
   dmu_cfg_D            0xa0010080   0x00000001
   qd_ac                0xa0024000   0x00000000
nightly-fx1/admin(config)#
```

The following is sample output from the **show np 1 interface-vlan** command in single mode:

```
hostname# sh np 1 interface-vlan 1

WARNING: Vlan is shared by multiple contexts
-------------------------------------------------------------------------------
                    Interface Statistics Counters (NP-1)
-------------------------------------------------------------------------------
Vlan Number                          : 1
Total Number of Packets RCV          : 0
Total Number of Packets TX           : 0
Total Number of Bytes RCV            : 0
Total Number of Bytes TX             : 0
Total Number of Packets Dropped      : 0
hostname#
```

The following is sample output from the **show np 1 mac** command in single mode:

```
hostname# sh np 1 mac
Number of mac-address entries = 0
hostname#
```

The following is sample output from the **show np 1 mcast** command in single mode:

```
hostname# sh np 1 mcast
-------------------------------------------------------------------------------
             Fast Path Multicast Statistics Counters (NP-1)
-------------------------------------------------------------------------------
MULTICAST_DROP: Destination IP address not class_D    : 0
MULTICAST_DROP: OSPF not enabled                      : 0
MULTICAST_DROP: RIP not enabled                       : 0
MULTICAST_DROP: Not UDP packet                        : 0
MULTICAST_DROP: Leaf not active                       : 0
MULTICAST_DROP: Leaf marked for deletion              : 0
MULTICAST_DROP: Dest port equal to 0                  : 0
MULTICAST_CNT : Control packet sent to PC             : 0
MULTICAST_CNT : Data packet received                  : 0
MULTICAST_CNT : Data packet sent out                  : 0
```

```
MULTICAST_CNT : Look up miss                          : 0
MULTICAST_CNT : Look up hit                           : 0
MULTICAST_CNT : Sent to other NP                      : 0
MULTICAST_CNT : Sent to NP 3                          : 0
MULTICAST_CNT : IGMP update received                  : 0
MULTICAST_CNT : A200 packets received                 : 0
MULTICAST_CNT : Leaf insertion succesfull             : 0
MULTICAST_CNT : Duplicate_entry                       : 0
hostname#
```

The following is sample output from the **show np 1 route** command in single mode:

```
hostname# sh np 1 route
Number of routes = 0
hostname#
```

The following is sample output from the **show np 1 semaphore** command in single mode:

```
hostname# sh np 1 semaphore
Showing Semaphore Information for np 1
   ThreadNum  SemNum    SemVal       Valid  Pending
       0        0      0x02e09020      N       N
                1      0x00000000      N       N
       1        0      0x00000037      N       N
                1      0x00000000      N       N
       2        0      0x024381e8      Y       N
                1      0x00000000      N       N
       3        0      0x02e0d098      N       N
                1      0x00000000      N       N
       4        0      0x00000000      N       N
                1      0x00000000      N       N
       5        0      0x00000000      N       N
                1      0x00000000      N       N
       6        0      0x00000000      N       N
                1      0x00000000      N       N
       7        0      0x00000000      N       N
                1      0x00000000      N       N
       8        0      0x00000000      N       N
                1      0x00000000      N       N
       9        0      0x00000000      N       N
                1      0x00000000      N       N
      10        0      0x00000000      N       N
                1      0x00000000      N       N
      11        0      0x00000000      N       N
                1      0x00000000      N       N
      12        0      0x00000000      N       N
                1      0x00000000      N       N
      13        0      0x00000000      N       N
                1      0x00000000      N       N
      14        0      0x00000000      N       N
                1      0x00000000      N       N
      15        0      0x0282ae38      N       N
                1      0x00000000      N       N
      16        0      0x00000000      N       N
                1      0x00000000      N       N
      17        0      0x00000000      N       N
                1      0x00000000      N       N
      18        0      0x00000000      N       N
                1      0x00000000      N       N
      19        0      0x00000000      N       N
                1      0x00000000      N       N
      20        0      0x00000000      N       N
                1      0x00000000      N       N
```

```
      21        0      0x00000000      N       N
                1      0x00000000      N       N
      22        0      0x00000000      N       N
                1      0x00000000      N       N
      23        0      0x0282ae38      N       N
                1      0x00000000      N       N
      24        0      0x00000000      N       N
                1      0x00000000      N       N
      25        0      0x00000000      N       N
                1      0x00000000      N       N
      26        0      0x00000000      N       N
                1      0x00000000      N       N
      27        0      0x0282ae38      N       N
                1      0x00000000      N       N
      28        0      0x00000000      N       N
                1      0x00000000      N       N
      29        0      0x00000000      N       N
                1      0x00000000      N       N
      30        0      0x00000000      N       N
                1      0x00000000      N       N
      31        0      0x82812799      N       N
                1      0x00000000      N       N
hostname#
```

The following is sample output from the **show np 1 stats** command in single mode:

```
hostname# sh np 1 stats
------------------------------------------------------------------------------
             Fast Path 64 bit Global Statistics Counters (NP-1)
------------------------------------------------------------------------------
PKT_MNG: total packets (dot1q) rcvd               : 93605
PKT_MNG: total packets (dot1q) sent               : 0
PKT_MNG: total packets (dot1q) dropped            : 0
PKT_MNG: TCP packets received                     : 0
PKT_MNG: UDP packets received                     : 0
PKT_MNG: ICMP packets received                    : 0
PKT_MNG: ARP packets received                     : 80259
PKT_MNG: other protocol pkts received             : 0
PKT_MNG: default (no IP/ARP) dropped              : 0
SESS_MNG: sessions created                        : 0
SESS_MNG: sessions embryonic to active            : 0
SESS_MNG: sessions deleted                        : 0
SESS_MNG: session lookup hits                     : 0
SESS_MNG: session lookup misses                   : 0
SESS_MNG: embryonic lookup hits                   : 0
SESS_MNG: embryonic lookup misses                 : 0
------------------------------------------------------------------------------
             Fast Path 32 bit Global Statistics Counters (NP-1)
------------------------------------------------------------------------------
SESS_MNG: insert errors                           : 0
SESS_MNG: embryonic to active errors              : 0
SESS_MNG: delete errors                           : 0
PKT_MNG: packets to NP-3                          : 0
PKT_MNG: packets from NP-3                        : 1795
PKT_MNG: packets to FWSM                          : 1794
PKT_MNG: packets from FWSM                        : 0
PKT_MNG: packets sent to other blade              : 0
PKT_MNG: packets rcv from other blade             : 0
PKT_MNG: pkt drop (l2 checks)                     : 13346
PKT_MNG: pkt drop (l3 checks)                     : 0
PKT_MNG: pkt drop (l4 checks)                     : 0
PKT_MNG: pkt drop (rate limiting)                 : 0
PKT_MNG: pkt drop (A200)                          : 0
LU_MNG: UDP packets sent by FP ok                 : 0
```

```
LU_MNG: TCP packets sent by FP ok                  : 0
LU_MNG: LU packets sent by SP ok                   : 0
LU_MNG: LU packets sent errors                     : 0
LU_MNG: UDP packets received for FP ok             : 0
LU_MNG: TCP packets received for FP ok             : 0
LU_MNG: LU packets received for SP ok              : 0
LU_MNG: LU packets received errors                 : 0
LU_MNG: LU packets redirected to NP3               : 0
LU_MNG: LU packets returned by NP3                 : 0
TLV_MNG: indications sent                          : 0
TLV_MNG: wrong tlv type (pkt dropped)              : 0
DBG_MNG: delete indications sent                   : 0
DBG_MNG: TLV4 received                             : 0
DBG_MNG: embryonic leaves deleted                  : 0
RTL_MNG: Route Lookup miss (pkt drop)              : 0
RTL_MNG: ARP Lookup miss                           : 0
RTL_MNG: MAC Relearns forced                       : 0
RTL_MNG: MAC Relearns forced aborted               : 0
AGE_MNG: Aging threads launched                    : 2099132
AGE_MNG: Aging threads aborted                     : 0
AGE_MNG: Aging ropes completed                     : 524783
AGE_MNG: Aging Errors (no flag set)                : 0
AGE_MNG: Aging Errors (no timeout set)             : 0
PKT_MNG: PKT_DROP_DHCP_INGR                        : 0
PKT_MNG: PKT_DROP_MULTIC_BROADC_INGR               : 0
PKT_MNG: PKT_DROP_A200_INGR                        : 0
PKT_MNG: PKT_DROP_ARP_INGR                         : 80259
PKT_MNG: PKT_DROP_A300_INGR                        : 0
PKT_MNG: PKT_DROP_NOT_DOT1Q_INGR                   : 2130195
PKT_MNG: PKT_DROP_A200_EGR                         : 0
PKT_MNG: PKT_DROP_A200_EMBR_LEAF_NON_ACTIVE        : 0
PKT_MNG: PKT_DROP_A200_EMBR_LEAF_MARK_DEL          : 0
PKT_MNG: PKT_DROP_A200_NAT_LEAF_NON_ACTIVE         : 0
PKT_MNG: PKT_DROP_A200_NAT_LEAF_MARK_DEL           : 0
PKT_MNG: PKT_DROP_A200_TLV_UPDATE_LEAF_NON_ACTIVE  : 0
PKT_MNG: PKT_DROP_A200_TLV_UPDATE_LEAF_MARK_DEL    : 0
PKT_MNG: PKT_DROP_A200_TLV_DEL_LEAF_NON_ACTIVE     : 0
PKT_MNG: PKT_DROP_A200_TLV_DEL_LEAF_MARK_DE        : 0
PKT_MNG: PKT_DROP_A200_LINK_DATA_CH_FAIL           : 0
PKT_MNG: PKT_DROP_A200_LEAF_INSERTION_FAIL         : 0
PKT_MNG: PKT_DROP_L4_FIXUP_ACK                     : 0
PKT_MNG: PKT_DROP_L4_FIXUP_SYN                     : 0
PKT_MNG: PKT_DROP_L4_FIXUP_RST                     : 0
PKT_MNG: PKT_DROP_L4_FIXUP_SYN_ACK                 : 0
RL_MNG: session miss packet dropped                : 0
RL_MNG: other protocol or ICMP dropped             : 0
RL_MNG: packet to PIX dropped                      : 0
RL_MNG: packet to Fixup-PC dropped                 : 0
RL_MNG: packet to Fixup-SP dropped                 : 0
PF_MNG: pause frames sent (x3)                     : 0
PKT_MNG: PKT_DROP_INVALID_GROUP_ID                 : 0
PKT_MNG: PKT_DROP_INVALID_PAIR_VLAN                : 0
PKT_MNG: PKT_DROP_L4_BAD_FLAGS                     : 0
PKT_MNG: PKT_DROP_L4_SEND_RST_A300                 : 0
PKT_MNG: PKT_DROP_L4_SEND_RST_ALREADY_RST          : 0
PKT_MNG: PKT_DROP_L4_SYN_ACK_SAME_DIREC_OF_SYN     : 0
PKT_MNG: PKT_DROP_L4_ACK_NOT_ACK_THE_SYN_ACK_INS   : 0
PKT_MNG: PKT_DROP_L4_ACK_NOT_ACK_THE_SYN_ACK_OUT   : 0
PKT_MNG: PKT_DROP_L4_ACK_RCV_IN_WRONG_DIRECTION    : 0
PKT_MNG: PKT_DROP_L4_BAD_CHECKSUM                  : 0
PKT_MNG: PKT_DROP_PIF_LOOKUP_FAIL                  : 0
PKT_MNG: PKT_DROP_BACK_TO_BACK_PACKET              : 0
CNT_NUMBER_FULL_OPEN_INDICATION_TO_BE_SENT         : 0
CNT_NUMBER_FULL_OPEN_INDICATION_SENT               : 0
```

```
IPv6 packet received                                : 0
IPv6 packet sent                                    : 0
IPv6 packet received from PC                        : 0
IPv6 packet sent to PC                              : 0
hostname#
```

The following is sample output from the **show np 1 status** command in single mode:

```
hostname# sh np 1 status
Showing the np 1 status
   NP             VALUE      STATUS
    1            0x00000005     Unknown Code
hostname#
```

The following is sample output from the **show np 1 syn-cookie** command in single mode:

```
hostname# sh np 1 syn-cookie
------------------------------------------------------------------------------
             Fast Path Syn Cookie Statistics Counters (NP-1)
------------------------------------------------------------------------------
SYN_COOKIE: Syn cookie secret wheel index                       : 94
SYN_COOKIE: Total number of SYNs intercepted                    : 0
SYN_COOKIE: Total number of ACKs intercepted                    : 0
SYN_COOKIE: Total number of ACKs dropped after lookup           : 0
SYN_COOKIE: Total number of ACKs successfully validated         : 0
SYN_COOKIE: Total number of ACKs Dropped: Secret Expired        : 0
SYN_COOKIE: Total number of ACKs Dropped: Invalid Sequence      : 0
SYN_COOKIE: Total number of Syn Cookie Entries inserted by NP3  : 0
SYN_COOKIE: ACKs dropped: Syn cookie ses not yet established    : 0
SYN_COOKIE: Leaf allocation failed                              : 0
SYN_COOKIE: Leaf insertion failed                               : 0
hostname#
```

Related Commands

Command	Description
show np block	Displays NP block information.
show np pc	Displays NP program counters.
show np acl-notification	Displays the status of NP access list notifications.

show np acl-notification

To display the status of NP access list notifications, use the **show np acl-notification** command in privileged EXEC mode.

show np acl-notification

Syntax Description

acl-notification	Displays the status of NP access list notifications.

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
3.1	This is command was introduced.

Examples

The following is sample output from the **show np acl-notification** command in single mode:

```
hostname# show np acl-notification
acl-notification on
hostname(config-ctx)#
```

Related Commands

Command	Description
show np	Displays extended NP information.
show np block	Displays NP block information.
show np pc	Displays the status of NP program counters.

show np block

To display the buffer information in all the network processors, use the **show np block** command in privileged EXEC mode.

show np block

Syntax Description

block	Shows the maximum and free blocks in each side (ingress or egress) in each NP and the amount of time thresholds were reached in each NP.

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
3.1	This is command was introduced.

Usage Guidelines

The **show np block** command displays the amount of time thresholds were reached in each NP.

Examples

The following is sample output from the **show np block** command in single mode:

```
hostname# show np block
                MAX   FREE   THRESH_0   THRESH_1   THRESH_2
NP1 (ingress)  32768  32768          0          0          0
    (egress)  521206 521206          0          0          0
NP2 (ingress)  32768  32768          0          0          0
    (egress)  521206 521206          0          0          0
NP3 (ingress)  32768  32768          0          0          0
    (egress)  521206 521206          0          0          0
hostname(config-ctx)#
```

Table 27-5 show np block Fields

Field	Description
NP*1*	The network processor number.
MAX	The maximum number of blocks the NP can use.

Table 27-5 show np block Fields (continued)

Field	Description
FREE	The number of free blocks remaining before the NP reaches its threshold.
THRESH_*0*	The thresholds are the limits a network processor can handle before it takes an action such as sending a pause frame, dropping new packets, or dropping the currently assembled packet. Threshold 0 is set as 48 buffers, Threshold 1 is set as 80 buffers, and Threshold 2 is set as 160 buffers.

Related Commands

Command	Description
show np	Displays extended NP information.
show np pc	Displays NP program counters.
show np acl-notification	Displays the status of NP access list notifications.

show np pc

To display the program counter in each of the 32 threads in all the network processors, use the **show np pc** command in privileged EXEC mode.

show np pc

Syntax Description

pc	Shows the maximum and free pcs in each side (ingress or egress) in each NP and the amount of time thresholds were reached in each NP.

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
3.1	This is command was introduced.

Examples

The following is sample output from the **show np pc** command in single mode:

```
hostname# show np pc
THREAD:PC(NP1/NP2/NP3)
 0:0000/0000/0000  1:0000/0000/0000  2:5c4a/45ff/0000  3:0000/0000/0000
 4:0000/0000/0000  5:0000/0000/0000  6:0000/0000/0000  7:0000/0000/0000
 8:0000/0000/0000  9:0000/0000/0000 10:0000/0000/0000 11:0000/0000/0000
12:0000/0000/0000 13:0000/0000/0000 14:0000/0000/0000 15:0000/0000/0000
16:0000/0000/0000 17:0000/0000/0000 18:0000/0000/0000 19:0000/0000/0000
20:0000/0000/0000 21:0000/0000/0000 22:0000/0000/0000 23:4628/0000/0000
24:0000/0000/0000 25:0000/0000/0000 26:0000/0000/0000 27:0000/0000/0000
28:0000/0000/0000 29:0000/0000/0000 30:0000/0000/0000 31:0000/0000/0000
hostname(config-ctx)#
```

Table 27-6 show np pc Fields

Field	Description
THREAD	Displays the program counter in each of the 32 threads in all the network processors

Related Commands

Command	Description
show np	Displays extended NP information.
show np block	Displays NP block information.
show np acl-notification	Activates NP access list notifications.

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
1.1(1)	This command was introduced (as **show ip ospf**).
3.1(1)	This command was changed from **show ip ospf** to **show ospf**.

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
1.1(1)	This command was introduced (as **show ip ospf border-routers**).
3.1(1)	This command was changed from **show ip ospf border-routers** to **show ospf border-routers**.

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 FWSM, 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
1.1(1)	This command was introduced (as **show ip ospf database**).
3.1(1)	This command was changed from **show ip ospf database** to **show ospf database**.

Usage Guidelines

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
1.1(1)	This command was introduced (as **show ip ospf flood-list**).
3.1(1)	This command was changed from **show ip ospf flood-list** to **show ospf flood-list**.

Usage Guidelines

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
1.1(1)	This command was introduced (as **show ip ospf interface**).
3.1(1)	This command was changed from **show ip ospf interface** to **show ospf interface**.

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
1.1(1)	This command was introduced (as **show ip ospf neighbor**).
3.1(1)	This command was changed from **show ip ospf neighbor** to **show ospf neighbor**.

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
1.1(1)	This command was introduced (as **show ip ospf request-list**).
3.1(1)	This command was changed from **show ip ospf request-list** to **show ospf request-list**.

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
1.1(1)	This command was introduced (as **show ip ospf retransmission-list**).
3.1(1)	This command was changed from **show ip ospf retransmission-list** to **show ospf retransmission-list**.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. 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
1.1(1)	This command was introduced (as **show ip ospf summary-address**).
3.1(1)	This command was changed from **show ip ospf summary-address** to **show ospf summary-address**.

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
1.1(1)	This command was introduced (as **show ip ospf virtual-links**).
3.1(1)	This command was changed from **show ip ospf virtual-links** to **show ospf virtual-links**.

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 Vlan101, 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 pager

To display the lines that are configured for screen paging, use the **show pager** command.

show pager

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
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the lines that are configured for screen paging:

```
fwsm(config)# show pager
pager lines 30
```

Related Commands

Command	Description
clear pager	Restores the pager command default settings.
pager	Sets the default number of lines on a page before the "---more---" prompt appears for Telnet sessions.

show pc conn

To display information about connections, address translation, and local host information that are maintained on the control-point, use the **show pc conn** command in privileged EXEC mode. This command also shows the number of TCP, UDP, and embryonic connections, as well as those connections most used.

show pc conn [**count**] | **local-host** | **xlate**

Syntax Description

count	Shows a count of the current active connections maintained on the control-point, along with a high water mark of most connections used on the control-pont.
local-host	Shows the total number of active TCP, UDP, and embryonic connections maintained on the control-point.
xlate	Shows the total number of active address translations maintained on the control-point.

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
2.3(1)	This command was introduced.

Usage Guidelines

All the connections that are being processed by the control-point on the FWSM display. These connections are being processed in software on the central CPU, not in hardware.

Examples

The following example shows how to display connection information:

```
hostname# show pc conn

2 in use, 10230 most used
UDP out 14.1.26.199:53 in 10.10.10.119:53 idle 0:00:00 flags
UDP out 14.1.26.199:53 in 10.10.10.119:53 idle 0:00:00 flags
```

Related Commands

Command	Description
show xlate	Shows translations.
show conn	Shows connection information.
show local-host	Shows IP addresses of local hosts.
set connection	Sets connection limits.

show perfmon

To capture information about the performance of the FWSM, use the **show perfmon** command in privileged EXEC configuration mode. To view the output, use the **show console-output** command.

show perfmon [detail]

Syntax Description

detail	Displays connection rates that you configure for a specified interval.

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
1.1(1)	This command was introduced.
3.2(1)	Added the **detail** keyword.

Usage Guidelines

The FWSM does not include a serial console port, but some messages are only displayed on a console port, including output from the **show perfmon** and **perfmon** commands. Use the **show output-console** command to view the console buffer, including the **show perfmon** command output.

The **perfmon** command allows you to monitor the FWSM performance. The **show perfmon** command allows you to display the information immediately. The **show perfmon detail** command allows you to display the connection and xlate setup rates in a new output section.

Examples

This example shows how to display information about the FWSM performance:

```
hostname# show perfmon
hostname# show console-output
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
```

This example shows how to display the connection and xlate setup rates.

```
hostname# show perfmon detail
hostname# show console-output
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
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
Xlates for 1 minute = 0/s; 5 minutes = 0/s
```

Related Commands

Command	Description
perfmon	Displays detailed performance monitoring information.
show console-output	Shows the console buffer.

show pim df

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

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

Syntax Description

if_name	The physical or logical interface name.
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.
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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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

The PIM implementation on the FWSM 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 FWSM.
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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The PIM implementation on the FWSM considers the FWSM 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 FWSM.

show pim join-prune statistic

To display PIM join/prune aggregation statistics, use the **show pim join-prune statistics** command in 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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

             Vlan38   0 /    0 /    0         0 /    0 /    0
             Vlan37   0 /    0 /    0         0 /    0 /    0
             Vlan36   0 /    0 /    0         0 /    0 /    0
             Vlan35   0 /    0 /    0         0 /    0 /    0
               Vlan   0 /    0 /    0         0 /    0 /    0
             Vlan34   0 /    0 /    0         0 /    0 /    0
             Vlan22   0 /    0 /    0         0 /    0 /    0
             Vlan20   0 /    0 /    0         0 /    0 /    0
               Vlan   0 /    0 /    0         0 /    0 /    0
            Vlan124   0 /    0 /    0         0 /    0 /    0
            Vlan136   0 /    0 /    0         0 /    0 /    0
            Vlan137   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 privileged EXEC mode.

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(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 FWSM considers the FWSM itself to be a PIM neighbor. Therefore, the FWSM interface is shown in the output of this command. The IP address of the FWSM 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 FWSM.

show pim range-list

To display range-list information for PIM, use the **show pim range-list** command in 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(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 processes

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

show processes [cpu-hog | memory | internals]

Defaults

By default this command displays the processes running on the FWSM.

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
3.1(1)	This command was introduced.

Usage Guidelines

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

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

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 and is accurate to within one millisecond, 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.

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 FWSM:

```
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 processes cpu

    MAXHOG            NUMHOG            LASTHOG             Process
--------------     ---------------     ---------------       ---------
      7720                4                110              Dispatch Unit
      7870              331               1010              Checkheaps
(other lines deleted for brevity)
      6170                1               6170              CTM message handle

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# sho proc 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 FWSM, 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
3.1(1)	Support for 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 acl-partition

To show the number of memory partitions in multiple context mode, the contexts assigned to each partition, and the number of rules used, use the **show resource acl-partition** command in privileged EXEC mode.

show resource acl-partition [*context*]

Syntax Description

context	Shows the partition to which a context is assigned.

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	N/A	N/A	—	—	•

Command History

Release	Modification
2.3(1)	This command was introduced.

Examples

The following is sample output from the **show resource acl-partition** command:

```
hostname# show resource acl-partition

Total number of configured partitions = 2
Partition #0
        Mode                        :exclusive
        List of Contexts          :bandn, borders
        Number of contexts    :2(RefCount:2)
        Number of rules           :0(Max:53087)
Partition #1
        Mode                        :non-exclusive
        List of Contexts          :admin, momandpopA, momandpopB, momandpopC
                                    momandpopD
        Number of contexts    :5(RefCount:5)
        Number of rules           :6(Max:53087)
```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
context	Configures a security context.
resource acl-partition	Determines the number of memory partitions for multiple context mode.

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	N/A	N/A	—	—	•

Command History

Release	Modification
2.2(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           35.00%
 Fixups [rate]              35000           35.00%
 Syslogs [rate]             10500           35.00%
 Conns                     305000           30.50%
 Hosts                      78842           30.07%
 IPsec                          7           35.00%
 SSH                           35           35.00%
 Telnet                        35           35.00%
 Xlates                     91749           34.99%
 All                    unlimited
```

Table 27-7 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 FWSM 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.

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     20.00%
                 silver             1      CA      17000      17000     10.00%
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     30.00%

Fixups [rate]    default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     10.00%
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     10.00%

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     20.00%
                 silver             1      CA       3000       3000     10.00%
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     30.00%

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      9.99%
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      9.99%

IPSec            default          all       C          5
                 gold               1       D          5          5     50.00%
                 silver             1      CA          1          1     10.00%
                 bronze             0      CA  unlimited
                 All Contexts:      3                            11    110.00%

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     10.00%
                 bronze             0      CA      11520
                 All Contexts:      3                         23040     10.00%

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 27-8 shows each field description.

Table 27-8 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 FWSM 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 FWSM 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 the resource is unlimited, this display is blank.

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 FWSM.

show resource partition

To view the current, startup, and default partition sizes, use the **show resource partition** command in global configuration mode.

show resource partition

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	•	•	—	—	•

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **show resource partition** command lets you plan how to resize memory partitions in multiple context mode using the **size** command. For more information about memory partitions, see the **resource acl-partition** command.

Examples

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

```
hostname(config)# show resource partition

                        Bootup     Current
 Partition   Default  Partition   Configured
  Number       Size       Size         Size
-----------+---------+----------+-----------
      0       19219      19219       19219
      1       19219      19219       19219
      2       19219      19219       19219
      3       19219      19219       19219
      4       19219      19219       19219
      5       19219      19219       19219
      6       19219      19219       19219
      7       19219      19219       19219
      8       19219      19219       19219
      9       19219      19219       19219
     10       19219      19219       19219
     11       19219      19219       19219
```

```
backup tree   19219      19219       19219
-----------+---------+----------+-----------
   Total     249847     249847      249847

Total Partition size - Configured size = Available to allocate
        249847       -     249847      =           0
```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
clear configure resource partition	Clears the current memory partition configuration.
resource acl-partition	Sets the total number of memory partitions.
resource partition	Customizes a memory partition.
resource rule	Reallocates rules between features globally for all partitions.
rule	Reallocates rules between features for a specific partition.
show resource acl-partition	Shows the current memory partition characteristics, including the sizes and allocated contexts.
show resource rule	Shows the current allocation of rules.
show running-config resource partition	Shows the current memory partition configuration.
size	Changes the size of a memory partition.

show resource rule

To show the total number of rules available, the default values, current rule allocation, and the absolute maximum number of rules you can allocate per feature, use the **show resource rule** command in privileged EXEC mode. There are a fixed number of rules available on the FWSM, so you might want to reallocate rules between features depending on usage. Features that use rules include access lists, inspections, AAA, and more.

show resource rule [**partition** [*number*]]

Syntax Description

number	(Optional) In multiple context mode, shows the rule allocation for a particular partition number.
partition	(Optional) In multiple context mode, shows the rule allocation per partition. You can override the global rule allocation for a specific partition if you enter the **rule** command. To view the global settings set by the **resource rule** command, use the **show resource rule** command without a partition number.

Defaults

If you do not specify the **partition** keyword, then the global settings 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
3.2(1)	This command was introduced.
4.0(1)	The **partition** and *number* arguments were added.

Usage Guidelines

Use the **resource rule** command to reallocate rules between features; in multiple context mode, the resource rule command sets the allocation globally for all partitions. Use the **rule** command to set the allocation for a specific partition. The **show resource rule** command lets you plan your resource allocation. In multiple context mode, this command shows the global setting for each partition. To see the actual rules allocated for a specific partition, use the **show resource rule partition** command. See the **resource acl-partition** command for more information about partitions.

You can also use the **show np 3 acl count** command to view the number of rules currently being used.

Examples

The following is sample output from the **show resource rule** command in single mode:

```
hostname(config)# show resource rule
```

```
             Default  Configured  Absolute
CLS Rule     Limit      Limit      Max
-----------+---------+----------+---------
 Policy NAT    1843      1843      10000
 ACL          74188     74188      74188
 Filter        2764      2764       5528
 Fixup         4147      4147      10000
 Est Ctl        460       460        460
 Est Data       460       460        460
 AAA           6451      6451      10000
 Console       1843      1843       3686
-----------+---------+----------+---------
 Total        92156     92156

Partition Limit - Configured Limit = Available to allocate
     92156      -     92156        =          0
```

The following is sample output from the **show resource rule partition** command in multiple mode:

```
hostname(config)# show resource rule partition 0

             Default  Configured  Absolute
CLS Rule     Limit      Limit      Max
-----------+---------+----------+---------
 Policy NAT     283       283        833
 ACL          10633     10633      10633
 Filter         425       425        850
 Fixup         1417      1417       2834
 Est Ctl         70        70         70
 Est Data        70        70         70
 AAA            992       992       1984
 Console        283       283        566
-----------+---------+----------+---------
 Total        14173     14173

Partition Limit - Configured Limit = Available to allocate
     14173      -     14173        =          0
```

Field descriptions for the **show resource rule** command are shown below:

Field	Description
CLS Rule	Shows the feature types that use rules.
Default Limit	Shows the default limit for each feature.
Configured Limit	Shows the limit you configured using the **resource rule** command.
Absolute Max	Shows the maximum limit you can assign to a feature using the **resource rule** command.
Policy NAT	Shows the default, configured, and maximum limits for policy NAT rules.
ACL	Shows the default, configured, and maximum limits for ACEs.
Filter	Shows the default, configured, and maximum limits for filter rules.
Fixup	Shows the default, configured, and maximum limits for inspect rules.

Field	Description
Est Ctl	Shows the default, configured, and maximum limits for **established** command control rules. **Note** The **established** command creates two types of rules, control and data. Both of these types are shown in the display, but you allocate both rules by setting the number of **established** commands; you do not set each rule separately. Be sure to double the **est** value in the **resource rule** command when comparing the total number of configured rules with the total number of rules shown in the **show resource rule** command.
Est Data	Shows the default, configured, and maximum limits for **established** command data rules. **Note** The **established** command creates two types of rules, control and data. Both of these types are shown in the display, but you allocate both rules by setting the number of **established** commands; you do not set each rule separately. Be sure to double the **est** value in the **resource rule** command when comparing the total number of configured rules with the total number of rules shown in the **show resource rule** command.
AAA	Shows the default, configured, and maximum limits for AAA rules.
Console	Shows the default, configured, and maximum limits for HTTP, Telnet, SSH, and ICMP rules.
Total	Shows the total number of rules for the system under the Default Limit column, and the total number of rules configured under the Configured Limit column.
Partition Limit - Configured Limit = Available to allocate	Shows the system limit (for multiple context mode, this is the partition limit) minus the number of rules you have configured so you can see the number of rules you can still allocate.

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
context	Configures a security context.
resource acl-partition	Sets the number of memory partitions for rules.
resource rule	Reallocates rules between features.
rule	Reallocates rules between features per partition.
show np 3 acl count	Shows the number of rules in use.
show resource acl-partition	Shows the contexts assigned to each memory partition and the number of rules used.

show resource types

To view the resource types for which the FWSM can limit usage per context, 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
2.2(1)	This command was introduced.

Examples

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

```
hostname# show resource types

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

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  IPSec           IPSec Mgmt Tunnels
  ASDM            ASDM Connections
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  MAC Addresses   MAC addresses
  All             All Resources
```

Related Commands

Command	Description
class	Creates a resource class.
context	Adds a security context.

Command	Description
limit-resource	Sets the resource limit for a class.
show resource allocation	Shows the resource allocation for each resource across all classes and class members.
show resource usage	Shows the resource usage of the FWSM.

show resource usage

To view the resource usage of the FWSM 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**]
[**resource** {*resource_name* | **all**} | **detail**] [**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 FWSM 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 allocation. • **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 *resource_name*	Shows the usage of a specific resource. Specify **all** (the default) for all resources. 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. • **hosts**—Hosts that can connect through the FWSM. • **ipsec**—IPSec sessions. • **mac-addresses**—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. • **ssh**—SSH sessions. • **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
2.2(1)	This command was introduced.

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
Fixups [rate]             270          535     100000(S)       0 Summary
U = Some contexts are unlimited and are not included in the total.
S = All contexts are unlimited; 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                1191228      1220084  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             26           27  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              0            0  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
chunk:est-sip               0            0  unlimited             0 admin
chunk:event-mgmt-m          0            0  unlimited             0 admin
chunk:event-mgmt-q          0            0  unlimited             0 admin
...

Telnet                      0            0          5             0 admin
SSH                         0            0          5             0 admin
ASDM                        0            0          5             0 admin
IPSec                       0            0          5             0 admin
Syslogs [rate]              0            0  unlimited             0 admin
aaa rate                    0            0  unlimited             0 admin
url filter rate             0            0  unlimited             0 admin
Conns                       0            0      20000             0 admin
Xlates                      0            0  unlimited             0 admin
tcp conns                   0            0  unlimited             0 admin
Hosts                       0            0  unlimited             0 admin
udp conns                   0            0  unlimited             0 admin
smtp-fixups                 0            0  unlimited             0 admin
Conns [rate]                0            0  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-intercept-rate          0            0  unlimited             0 admin
globals                     0            0  unlimited             0 admin
np-statics                  2            2  unlimited             0 admin
statics                     1            1  unlimited             0 admin
nats                        1            1  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           1            1         N/A              0 admin
policy-nat-rules             0            0         N/A              0 admin
fixup-rules                 32           32         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
Mac-addresses                0            0       65535              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 route

To display a default or static route for an interface, use the **show route** command in privileged EXEC mode.

show route [*interface_name ip_address netmask gateway_ip*]

Syntax Description

gateway_ip	(Optional) IP address of the gateway router (the next-hop address for this route).
interface_name	(Optional) Internal or external network interface name.
ip_address	(Optional) Internal or external network IP address.
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
1.1(1)	This command was introduced.

Examples

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

```
hostname(config)# show route
C    10.30.10.0 255.255.255.0 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
```

Related Commands

Command	Description
clear configure route	Removes the **route** commands from the configuration that do not contain the **connect** keyword.
route	Specifies a static or default route for the an interface.
show running-config route	Displays configured routes.

show route-inject

To display all the routes and NAT pools that have been injected, use the **show route-inject** command in privileged EXEC mode.

show route-inject

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
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show route-inject** command in privileged EXEC mode to display the routes and NAT pools that have been injected.

Examples

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

```
hostname(config)# show route-inject
Routes injected:
Address Mask Nexthop Proto Weight Vlan
-------------------------------------------------------
20.11.111.11
20.11.111.11 255.255.255.0
NATs injected:
Address Mask Nexthop Weight Vlan
-------------------------------------------------------
20.11.111.11 255.255.255.0
```

Related Commands

Command	Description
clear configure route-inject	Removes the routes/NAT pools that were injected into the MSFC routing tables. Additionally, removes the redistribute and route-inject configuration for the user context if you are in multi-mode or system context if in single routed mode.
debug route-inject	Enables debugging of the route-injections that have been configured on FWSM.
route-inject	Injects the connected and static routes and NAT pools configured on FWSM into the MSFC routing table.
show running-config route-inject	Displays the route-injection running configuration.