show pager through show route Commands

show pager

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

show pager

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.

Examples

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

```
hostname(config)# show pager
pager lines 0
```

Related Commands

Command	Description
clear configure pager	Removes the number of lines set to display in a Telnet session before the "---More---" prompt appears from the running configuration.
terinal pager	Sets the number of lines to display in a Telnet session before the "---More---" prompt appears. This command is not saved to the running configuration.
show running-config pager	Displays the number of lines set to display in a Telnet session before the "---More---" prompt appears in the running configuration.

show password encryption

To show the password encryption configuration settings, use the **show password encryption** command in privileged EXEC mode.

show password encryption

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.3(1)	This command was introduced.
8.4(1)	Allows you to show password encryption in user context.

Usage Guidelines

If the key has been saved using the **write memory** command, “saved” appears next to the key hash. If there is no key or it has been removed from the running configuration, “Not set” appears instead of the hash value.

Examples

The following is sample output from the **show password encryption** command:

```
hostname# show password encryption
Password Encryption: Enabled
Master key hash: 0x35859e5e 0xc607399b 0x35a3438f 0x55474935 0xbec1ee7d(not saved)
```

Related Commands

Command	Description
password encryption aes	Enables password encryption.
key config-key password-encrypt	Sets the pass phrase used for generating the encryption key.

show perfmon

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

show perfmon [**detail**]

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

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

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

Command History

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

Usage Guidelines

This command output does not display in a Telnet session.

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

Examples

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

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

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

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

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

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

Related Commands

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

show phone-proxy

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

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

Examples

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

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

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

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

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

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

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

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

Related Commands

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

show pim df

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command also displays the winner metric towards the RP.

Examples

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

```
hostname# show pim df
RP           Interface   DF Winner   Metrics

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

show pim group-map

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

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

Syntax Description

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

Defaults

Displays group-to-protocol mappings for all groups.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

The PIM implementation on the ASA 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 ASA.
pim rp-address	Configures the address of a PIM rendezvous point (RP).

show pim interface

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The PIM implementation on the ASA considers the ASA 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 ASA.

show pim join-prune statistic

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

show pim join-prune statistics [*if_name*]

Syntax Description

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

Defaults

If an interface is not specified, this command shows the join/prune statistics for all interfaces.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname# show pim join-prune statistic

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

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

Related Commands

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim neighbor

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

The PIM implementation on the ASA considers the ASA itself to be a PIM neighbor. Therefore, the ASA interface is shown in the output of this command. The IP address of the ASA 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 ASA.

show pim range-list

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

show pim range-list [*rp_address*]

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

show pim topology

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

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

Syntax Description

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

Defaults

Topology information for all groups and sources is shown.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

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

```
hostname# show pim topology

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

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

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

Related Commands

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

show pim topology reserved

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

show pim topology reserved

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# show pim topology reserved

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

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

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

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show pim topology route-count

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

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

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname# show pim topology route-count

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

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show pim traffic

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

show pim traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

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

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

Related Commands

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim tunnel

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

show pim tunnel [*if_name*]

Syntax Description

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

Defaults

If an interface is not specified, this command shows the PIM tunnel information for all interfaces.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
hostname# show pim tunnel

Interface     RP Address Source Address

Encapstunnel0 10.1.1.1   10.1.1.1
Decapstunnel0 10.1.1.1   -
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show port-channel

To display EtherChannel information in a detailed and one-line summary form or to display the port and port-channel information, use the **show port-channel** command in privileged EXEC mode.

show port-channel [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

Syntax Description

brief	(Default) Shows a brief display.
channel_group_number	(Optional) Specifies the EtherChannel channel group number, between 1 and 48, and only shows information about this channel group.
detail	(Optional) Shows a detailed display.
port	(Optional) Shows information for each interface.
protocol	(Optional) Shows the EtherChannel protocol, such as LACP if enabled.
summary	(Optional) Shows a summary of port-channels.

Command Default

The default is **brief**.

Command Modes

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

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

Command History

Release	Modification
8.4(1)	We introduced this command.

Examples

The following is sample output from the **show port-channel** command:

```
hostname# show port-channel
        Channel-group listing:
        -----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
```

The following is sample output from the **show port-channel summary** command:

```
hostname# show port-channel summary
```

```
Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1             LACP    Gi3/1   Gi3/2   Gi3/3
```

The following is sample output from the **show port-channel detail** command:

```
hostname# show port-channel detail
       Channel-group listing:
       -----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x0       0x1      0x306       0x3d


Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------------
```

```
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d


Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
--------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-----------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

The following is sample output from the **show port-channel port** command:

```
hostname# show port-channel port
        Channel-group listing:
        ----------------------

Group: 1
----------
        Ports in the group:
        -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
--------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-----------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d


Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
```

```
Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x0       0x1      0x303       0x3d


Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x0       0x1      0x302       0x3d
```

The following is sample output from the **show port-channel protocol** command:

```
hostname# show port-channel protocol
        Channel-group listing:
        -----------------------


Group: 1
----------
Protocol: LACP
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.

Command	Description
show lacp	Displays LACP information such as traffic statistics, system identifier, and neighbor details.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

show port-channel load-balance

For EtherChannels, to display the current port-channel load-balance algorithm, and optionally to view the member interface selected for a given set of parameters, enter this command in privileged EXEC mode.

show port-channel *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **mac** | **l4port** | **mixed** | **vlan-only** *number*} *parameters*]

Syntax Description

channel_group_number	Specifies the EtherChannel channel group number, between 1 and 48.
hash-result	(Optional) Shows the member interface chosen after hashing values you enter for the current load-balancing algorithm.
ip	(Optional) Specifies IPv4 packet parameters.
ipv6	(Optional) Specifies IPv6 packet parameters.
l4port	(Optional) Specifies port packet parameters.
mac	(Optional) Specifies MAC addresss packet parameters.
mixed	(Optional) Specifies a combination of IP or IPv6 parameters, along with ports and/or the VLAN ID.
parameters	(Optional) Packet parameters, depending on the type. For example, for **ip**, you can specify the source IP address, the destination IP address, and/or the VLAN ID.
vlan-only	(Optional) Specifies the VLAN ID for a packet.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(1)	We introduced this command.

Usage Guidelines

By default, the ASA balances the packet load on interfaces according to the source and destination IP address (**src-dst-ip**) of the packet. To change the algorithm, see the **port-channel load-balance** command.

This command lets you view the current load-balancing algorithm, but, with the **hash-result** keyword, also lets you test which member interface will be chosen for a packet with given parameters. This command only tests against the current load-balancing algorithm. For example, if the algorithm is src-dst-ip, then enter the IPv4 or IPv6 source and destination IP addresses. If you enter other arguments not used by the current algorithm, they are ignored, and the unentered values actually used by the algorithm default to 0. For example, if the algorithm is vlan-src-ip, then enter:

```
show port-channel 1 load-balance hash-result ip source 10.1.1.1 vlan 5
```

If you enter the following, then the vlan-src-ip algorithm assumes a source IP address of 0.0.0.0 and VLAN 0, and ignores the values you enter:

```
show port-channel 1 load-balance hash-result l4port source 90 destination 100
```

Examples

The following is sample output from the **show port-channel 1 load-balance** command:

```
hostname# show port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
       src-dst-ip

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
 IPv4: Source XOR Destination IP address
 IPv6: Source XOR Destination IP address
```

The following is sample output from the **show port-channel 1 load-balance hash-result** command, where the entered parameters match the current algorithm (src-dst-ip):

```
hostname# show port-channel 1 load-balance hash-result ip source 10.1.1.1 destination
10.5.5.5
Would select GigabitEthernet2/1 based on algorithm src-dst-ip
```

The following is sample output from the **show port-channel 1 load-balance hash-result** command, where the entered parameters do not match the current algorithm (src-dst-ip), and the hash uses 0 values:

```
hostname# show port-channel 1 load-balance hash-result l4port source 5
Would select GigabitEthernet3/2 of Port-channel1 based on algorithm src-dst-ip
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.

Command	Description
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.

show power inline

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

show power inline

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname# show power inline

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

Table 53-1 shows each field description:

Table 53-1 show power inline Fields

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

Related Commands

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

show priority-queue statistics

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

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

Syntax Description

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

Defaults

If you omit the interface name, this command shows priority-queue statistics for all configured interfaces.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows the use of the **show priority-queue statistics** command for the interface named test, and the command output. In this output, BE indicates the best-effort queue, and LLQ represents the low-latency queue:

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type      = BE
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0

Queue Type      = LLQ
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
hostname#
```

Related Commands

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

show processes

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

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

Syntax Description

cpu-hog	Shows number and detail of processes that are hogging the CPU (that is, using the CPU for more than 100 milliseconds).
cpu-usage	Shows percentage of CPU used by each process for the last 5 seconds, 1 minute and 5 minutes.
internals	Shows internal details of each process.
memory	Shows memory allocation for each process.
non-zero	(Optional) Shows processes with non-zero CPU usage.
sorted	(Optional) Shows sorted CPU usage for processes.

Defaults

By default, this command displays the processes running on the ASA.

Command Modes

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

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

Command History

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

Usage Guidelines

Processes are lightweight threads that require only a few instructions. The **show processes** commands display a list of the processes that are running on the ASA, as follows:

Command	Data Displayed	Description
show processes	PC	Program counter.
show processes	Stack Pointer	Stack pointer.
show processes	STATE	Address of thread queue.

Command	Data Displayed	Description
show processes	Runtime	Number of milliseconds that the thread has been running based on CPU clock cycles. The accurracy is within one millisecond for complete and accurate accounting of process CPU usage based on CPU clock cycles (<10ns resolution) instead of clock ticks (10ms resolution).
show processes	SBASE	Stack base address.
show processes	Stack	Current number of bytes in use and the total size of the stack.
show processes	Process	Function of the thread.
show processes cpu-usage	MAXHOG	Maximum CPU hog runtime in milliseconds.
show processes cpu-usage	NUMHOG	Number of CPU hog runs.
show processes cpu-usage	LASTHOG	Last CPU hog runtime in milliseconds.
show processes cpu-usage	PC	Instruction pointer of the CPU hogging process.
show processes cpu-usage	Traceback	Stack trace of the CPU hogging process. The traceback can have up to 14 addresses.
show processes internals	Invoked Calls	Number of times the scheduler ran the process.
show processes internals	Giveups	Number of times the process yielded the CPU back to the scheduler.

Use the **show processes cpu-usage** command to narrow down a particular process on the ASA that might be using the CPU of the ASA. You can use the **sorted** and **non-zero** commands to further customize the output of the **show processes cpu-usage** command.

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

- Consumption of 100% of the CPU.
- Percentage of CPU used by each thread, determined by comparing the runtime delta of a thread to the total runtime delta.

Examples

The following example shows how to display a list of processes that are running on the ASA:

```
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
```

The following example shows how to display the percentage of CPU used by each process:

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

The following example shows how to display the number and detail of processes that are hogging the CPU:

```
hostname(config)# show processes cpu-hog
Process:      Unicorn Admin Handler, NUMHOG: 1, MAXHOG: 13, LASTHOG: 13
LASTHOG At:   08:30:15 PST Jan 20 2011
PC:           0x08413a62
Call stack:   0x084f6c5d  0x08412cc3  0x08407a85  0x0806e0ea  0x08a4b17d  0x0806e0ea
0x0849bffd
              0x084950cd  0x0849530c  0x08495636  0x0849bc59  0x080680cc

(other lines deleted for brevity)
```

The following example shows how to display the memory allocation for each process:

```
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
```

The following example shows how to display the internal details of each process:

```
hostname# show processes internals

     Invoked      Giveups  Process
           1            0  block_diag
    19108445     19108445  Dispatch Unit
           1            0  CF OIR
           1            0  Reload Control Thread
           1            0  aaa
           2            0  CMGR Server Process
           1            0  CMGR Timer Process
           2            0  dbgtrace
          69            0  557mcfix
    19108019     19108018  557poll
           2            0  557statspoll
           1            0  Chunk Manager
         135            0  PIX Garbage Collector
           6            0  route_process
           1            0  IP Address Assign
```

```
            1            0  QoS Support Module
            1            0  Client Update Task
         8973         8968  Checkheaps
            6            0  Session Manager
          237          235  uauth
(other lines deleted for brevity)
```

show quota management-session

To show statistics for the current management session:, use the **show quota management-session** command in privileged EXEC mode.

show quota management-session

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
9.1(2)	This command was introduced.

Usage Guidelines

This command shows the following statistics for the current management session:

- Limit
- Warning level
- Current count
- High water mark
- Number of warnings generated
- Number of errors generated

Examples

The following example shows statistics for the current management session:

```
hostname# show quota management-session
quota management-session limit 250
quota management-session warning level 225
quota management-session level 1
quota management-session high water 1
quota management-session errors 0
quota management-session warnings 0
```

Related Commands

Command	Description
show running-config quota management-session	Shows the current value of the management session quota.
quota management-session	Sets the number of simultaneous ASDM, SSH, and Telnet sessions allowed on the device.

show reload

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

show reload

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

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

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

Related Commands

Command	Description
reload	Reboots and reloads the configuration.

show resource allocation

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

show resource allocation [**detail**]

Syntax Description

detail	Shows additional information.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.
9.0(1)	A new resource class, routes, was created to set the maximum number of routing table entries in each context. New resource types, vpn other and vpn burst other, were created to set the maximum number of site-to-site VPN tunnels in each context.

Usage Guidelines

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

Examples

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

```
hostname# show resource allocation
Resource                     Total       % of Avail
 Conns [rate]                35000           N/A
 Inspects [rate]             35000           N/A
 Syslogs [rate]              10500           N/A
 Conns                      305000           30.50%
 Hosts                       78842           N/A
 SSH                            35           35.00%
 Telnet                         35           35.00%
 Routes                      25000           0.00%
 Xlates                      91749           N/A
```

```
Other VPN Sessions            20           2.66%
Other VPN Burst               20           2.66%
All                    unlimited
```

Table 53-2 shows each field description.

Table 53-2 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 ASA converts the percentage to an absolute number for this display.
% of Avail	The percentage of the total system resources that is allocated across all contexts, if available. If a resource does not have a system limit, this column shows N/A.

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

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

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

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

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

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

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

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

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

mac-addresses    default          all       C      65535
                 gold               1       D      65535      65535    100.00%
                 silver             1      CA       6553       6553      9.99%
```

```
bronze              0       CA       3276
All Contexts:       3                         137623    209.99%
```

Table 53-3 shows each field description.

Table 53-3 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 ASA 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 ASA converts the percentage to an absolute number for this display.
Total	The total amount of the resource that is allocated across all contexts in the class. The amount is an absolute number of concurrent instances or instances per second. If the resource is unlimited, this display is blank.
% of Avail	The percentage of the total system resources that is allocated across all contexts in the class, if available. If the resource is unlimited, this display is blank. If the resource does not have a system limit, this column shows N/A.

Related Commands

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

show resource types

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

show resource types

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command shows additional resource types that you can manage for each context.
9.0(1)	A new resource class, routes, was created to set the maximum number of routing table entries in each context. New resource types, vpn other and vpn burst other, were created to set the maximum number of site-to-site VPN tunnels in each context.

Examples

The following sample display shows the resource types:

```
hostname# show resource types

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

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  Mac-addresses   MAC Address table entries
  ASDM            ASDM Connections
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  Routes          Routing Table Entries
  Other-vpn       Other VPN licenses
```

```
Other-vpn-burst Allowable burst for Other VPN licenses
All             All Resources
```

Related Commands

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

show resource usage

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

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

Syntax Description

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

resource [**rate**] *resource_name*	Shows the usage of a specific resource. Specify **all** (the default) for all resources. Specify **rate** to show the rate of usage of a resource. Resources that are measured by rate include **conns**, **inspects**, and **syslogs**. You must specify the **rate** keyword with these resource types. The conns resource is also measured as concurrent connections; only use the **rate** keyword to view the connections per second. Resources include the following types: • **asdm**—ASDM management sessions. • **conns**—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • **inspects**—Application inspections. • **hosts**—Hosts that can connect through the ASA. • **mac-addresses**—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. • **routes—**Routing Table entries. • **ssh**—SSH sessions. • **syslogs**—System log messages. • **telnet**—Telnet sessions. • (Multiple mode only) **VPN Other**—Site-to-site VPN sessions. • (Multiple mode only) **VPN Burst Other**—Site-to-site VPN burst 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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command shows the denied resources, because you can limit the resources for each context.
9.0(1)	A new resource class, routes, was created to set the maximum number of routing table entries in each context. New resource types, vpn other and vpn burst other, were created to set the maximum number of site-to-site VPN tunnels in each context.

Examples

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

```
hostname# show resource usage context admin

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

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

```
hostname# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
Conns [rate]              270          535      42200       1704 Summary
Inspects [rate]           270          535     100000(S)       0 Summary
Other VPN Sessions          0           10         10        740 Summary
Other VPN Burst             0           10         10        730 Summary
U = Some contexts are unlimited and are not included in the total.
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

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

```
hostname# show resource usage system

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

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

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

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

...

Telnet                      0            0          5              0 admin
SSH                         1            1          5              0 admin
ASDM                        0            1          5              0 admin
Syslogs [rate]              0           68  unlimited              0 admin
aaa rate                    0            0  unlimited              0 admin
url filter rate             0            0  unlimited              0 admin
Conns                       1            6  unlimited              0 admin
Xlates                      0            0  unlimited              0 admin
tcp conns                   0            0  unlimited              0 admin
Hosts                       2            3  unlimited              0 admin
Other VPN Sessions          0           10        750            740 admin
Other VPN Burst             0           10        750            730 admin
udp conns                   0            0  unlimited              0 admin
smtp-fixups                 0            0  unlimited              0 admin
Conns [rate]                0            7  unlimited              0 admin
establisheds                0            0  unlimited              0 admin
pps                         0            0  unlimited              0 admin
syslog rate                 0            0  unlimited              0 admin
bps                         0            0  unlimited              0 admin
Fixups [rate]               0            0  unlimited              0 admin
non tcp/udp conns           0            0  unlimited              0 admin
tcp-intercepts              0            0  unlimited              0 admin
globals                     0            0  unlimited              0 admin
np-statics                  0            0  unlimited              0 admin
statics                     0            0  unlimited              0 admin
nats                        0            0  unlimited              0 admin
ace-rules                   0            0        N/A              0 admin
aaa-user-aces               0            0        N/A              0 admin
filter-rules                0            0        N/A              0 admin
est-rules                   0            0        N/A              0 admin
aaa-rules                   0            0        N/A              0 admin
console-access-rul          0            0        N/A              0 admin
policy-nat-rules            0            0        N/A              0 admin
fixup-rules                 0            0        N/A              0 admin
aaa-uxlates                 0            0  unlimited              0 admin
CP-Traffic:IP               0            0  unlimited              0 admin
CP-Traffic:ARP              0            0  unlimited              0 admin
CP-Traffic:Fixup            0            0  unlimited              0 admin
CP-Traffic:NPCP             0            0  unlimited              0 admin
```

```
CP-Traffic:Unknown          0            0  unlimited            0 admin
```

Related Commands

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

show rip database

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
hostname# show rip database

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

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

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

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

Related Commands

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

show route

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

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

Syntax Description

cluster	(Optional) Displays the routing information base (RIB) epoch number (sequence number), the current timer value, and the network descriptor block epoch number (sequence number).
failover	(Optional) Displays the current sequence number of the routing table and routing entries after failover has occurred, and a standby unit becomes the active unit.
interface_name	(Optional) Limits the display to route entries that use the specified interface.
ip_address	(Optional) Limits the display to routes to the specified destination.
netmask	(Optional) Defines the network mask to apply to the specified destination.
static	(Optional) Limits the display to static routes.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.4(1)	The **failover** keyword was added. The output shows the RIB epoch number (sequence number), current timer value, and network descriptor block epoch number (sequence number).
9.0(1)	The **cluster** keyword was added. Applies to the dynamic routing protocols (EIGRP, OSPF, and RIP) and is only available on the ASA 5580 and 5585-X.

Usage Guidelines

The **show route** command provides output similar to the **show ipv6 route** command, except that the information is IPv4-specific.

Note The **clustering** and **failover** keywords do not appear unless these features are configured on the ASA.

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

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

Examples

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

```
hostname# show route

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

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

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

The following is sample output of the **show route** command on the ASA 5505. The output displays the internal loopback address, which is used by the VPN hardware client for individual user authentication.

```
hostname(config)# show route

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

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

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

The following is sample output of the **show route failover** command, which shows the synchronization of OSPF and EIGRP routes to the standby unit after failover:

```
hostname(config)# show route failover

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

```
Gateway of last resort is 10.86.194.1 to network 0.0.0.0
Routing table sequence number 1
Reconvergence timer 00.20 (Running)

S    10.10.10.0 255.0.0.0 [1/0] via 10.10.10.1, mgmt, seq 1
                       [1/0] via 10.10.10.2, mgmt, seq 1
D    209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 1

O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 0

D   10.65.68.220 255.255.255.255 [1/0] via 10.76.11.1, mgmt, seq 1
```

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

```
hostname(cfg-cluster)# show route cluster

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

Gateway of last resort is not set

Routing table seq num 2
Reconvergence timer expires in 52 secs

C    70.0.0.0 255.255.255.0 is directly connected, cluster, seq 1
C    172.23.0.0 255.255.0.0 is directly connected, tftp, seq 1
C    200.165.200.0 255.255.255.0 is directly connected, outside, seq 1
C    198.51.100.0 255.255.255.0 is directly connected, inside, seq 1
O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 2
D   209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 2
```

Note When you use the **show ip route** command in the Cisco IOS, the **longer-prefix** keyword is available. When you use this keyword in the Cisco IOS, the route is only displayed if the specified network and mask pair match.

On the ASA, the **longer-prefix** keyword is the default behavior for the **show rout**e command; that is, no additional keyword is needed in the CLI. Because of this, you cannot see the route when you type **ip**. To obtain the supernet route, the mask value needs to be passed with the IP address.