show p – show r

show packet tracer

To display information about the pcap trace output, use the **show packet tracer** command.

show packet-tracer pcap trace [**packet-number** *number* | **summary** | **detailed** | **status**]

Syntax Description

packet-number	(Optional) Displays trace output for a single packet in pcap.
summary	(Optional) Displays pcap summary.
detailed	(Optional) Displays trace output for all packets in pcap.
status	(Optional) Displays the current execution state of pcap trace.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.17.1	The command was enhanced to include output of pcap trace.

Usage Guidelines

The **show packet-tracer** command shows the packet tracer output. The **pcap trace** command allows you to display the trace buffer output of the most recently run packet-tracer on a PCAP file.

Examples

The following is sample output for the **show packet-tracer pcap trace summary** command:

```
ciscoasa# show packet-tracer pcap trace summary
      1: 02:38:01.265123       6.1.1.100.51944 > 9.1.1.100.80: S 542888804:542888804(0) win
 29200 <mss 1460,sackOK,timestamp 2526545680 0,nop,wscale 7>
      2: 02:38:01.271317       9.1.1.100.80 > 6.1.1.100.51944: S 2281169942:2281169942(0)
ack 542888805 win 28960 <mss 1380,sackOK,timestamp 2526520070 2526545680,nop,wscale 7>
      3: 02:38:01.271638       6.1.1.100.51944 > 9.1.1.100.80: . ack 2281169943 win 229
<nop,nop,timestamp 2526545682 2526520070>

               Total packets: 3
       Packets replayed: 3
       Result: Allow
       Start time: Mar 28 04:51:54
```

```
  Total time taken: 10247935ns
show packet-tracer pcap trace packet-number 1 detailed
1: 02:38:01.265123 0050.56a9.81e5 0050.56a9.60e1 0x0800 Length: 74
 6.1.1.100.51944 > 9.1.1.100.80: S [tcp sum ok] 542888804:542888804(0) win 29200 <mss
1460,sackOK,timestamp 2526545680 0,nop,wscale 7> (DF) (ttl 64, id 54388)
 Phase: 1
 Type: ACCESS-LIST
 Subtype:
 Result: ALLOW
 Time Spent: 12345 ns
 Config:
 Implicit Rule
 Additional Information:
 Forward Flow based lookup yields rule:
  in  id=0x154523db3ce0, priority=1, domain=permit, deny=false
                hits=92, user_data=0x0, cs_id=0x0, l3_type=0x8
                src mac=0000.0000.0000, mask=0000.0000.0000
                dst mac=0000.0000.0000, mask=0100.0000.0000
                input_ifc=inside, output_ifc=any
 …
 …
```

Related Commands

Command	Description
packet tracer	Generates a 5-to-6 tuple packet against a firewall's current configurations

show packet-statistics

To display information about any packet drops on the Secure Firewall 3100, use the **show packet-statistics** command.

show packet-statistics *interface_id* [**brief**]

Syntax Description

interface_id	Interface ID for which the statistics are displayed.
brief	(Optional) Displays the output excluding the zero counter values.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.18(1)	This command was introduced.

Usage Guidelines

The **show packet-statistics** command collates and displays packet loss data from several sources in the operating system. The output helps to identify where the packets were dropped. This command consolidates the output of the following commands:

- FXOS:
  - **show portmanager counters ethernet**
  - **show queuing interface ethernet**
  - **show portmanager counters internal**
  - **show queuing interface internal**
  - **show portmanager switch counters packet-trace**
  - FPGA: **show npu-accel statistics**
  - ASA:
    - **show interface detail**
    - **show asp drop**

The consolidated output is in the sequence of the data path when traffic reach a device. In addition, the output is not broken or interrupted by other CLIs' output.

Examples

The following is sample output for the **show packet-statistics** command:

```
ciscoasa# show packet-statistics Ethernet 1/1
============= show portmanager counters Ethernet 1 1 ==============
Good Octets Received : 66882
Bad Octets Received : 0
MAC Transmit Error : 0
…
…
============= show queuing interface Ethernet 1 1 ==============
Queue Traffic-type Scheduler-type oper-bandwidth Destination
-------------------------------------------------------------------------------
3 Data WRR 100 Application
4 CCL-CLU SP 0 Application
5 BFD SP 0 Application
…
…
…
============= show portmanager counters Internal 1 1 ==============
Good Octets Received : 3770
Bad Octets Received : 0
MAC Transmit Error : 0
…
…
============= show queuing interface Internal 1 1 ==============
Queue Traffic-type Scheduler-type oper-bandwidth Destination
-------------------------------------------------------------------------------
3 Data WRR 100 Application
4 CCL-CLU SP 0 Application
5 BFD SP 0 Application
…
…
====================== show portmanager switch counters packet-trace ======================
Counter Source port- 0/0 Destination port- 0/0
---------------------- -------------------- --------------------
goodOctetsRcv --- ---
badOctetsRcv --- ---
Ingress counters
gtBrgInFrames 5 5
gtBrgVlanIngFilterDisc 0 0
…
…
====================== show npu-accel statistics ======================
module: kc50-pcie, pipe: 0
--------------------------
reg_pcie_rcv_reg_access_rd_tlp_cnt = 1312987327
reg_pcie_rcv_reg_access_wr_tlp_cnt = 227526828
…
…
====================== show interface detail ======================
Interface Ethernet1/1 "", is admin down, line protocol is down
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
Auto-Duplex, Auto-Speed
Available but not configured via nameif
MAC address f87a.410e.5994, MTU not set
…
…
```

```
====================== show asp drop ======================
Frame drop:
Slowpath security checks failed (sp-security-failed) 18
FP L2 rule drop (l2_acl) 118
Interface is down (interface-down) 11
Last clearing: Never
```

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was added.

Examples

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

```
ciscoasa(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.
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.
terminal 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 path-monitoring

To display information about the path monitoring output, use the **show path monitoring** command.

show path-monitoring [**interface** *name*] [**detail**]

Syntax Description

Interface*name*	Interface for which the path monitoring metric is displayed
detail	(Optional) Displays detailed information about path monitoring metrics.

Command Default

No default behavior or values.

Command History

Release	Modification
9.18(1)	The command was introduced to display the path monitoring details for a specified interface.

Usage Guidelines

The **show path-monitoring** command shows the path monitoring output for the specified egress interface.

Examples

The following is sample output for the **show path-monitoring** command for *outside 1* interface:

```
ciscoasa# show path-monitoring interface outside1
Interface: outside1
Remote peer: 90.2.1.1
    Version: 14275
    Remote peer reachable: Yes
    RTT average: 1407 microsecond(s)
    Jitter: 1218 microsecond(s)
    Packet loss: 0%
    MOS: 4.40
    Last updated: 1 second(s) ago
```

The following is sample output for the **show path-monitoring detail** command for *outside 1* interface:

```
ciscoasa#
firepower# show path-monitoring interface outside1 detail
Interface: outside1
Remote peer: 90.2.1.1
    Version: 14275
    Remote peer reachable: Yes
    RTT average: 1407 microsecond(s)
    Jitter: 1218 microsecond(s)
    Packet loss: 0%
    MOS: 4.40
    Last updated: 8 second(s) ago

    Internal data:
        Total probes sent: 418553
        Total probes pending: 0
        Current probes pending: 0
        Current RTT sum: 51674
        Current RTT square sum: 154410282
```

```
Flags: 0x2
Current queue index: 14
Index:  0, Timestamp:              0, RTT:     962
Index:  1, Timestamp:              0, RTT:    1096
Index:  2, Timestamp:              0, RTT:    1056
Index:  3, Timestamp:              0, RTT:    1457
Index:  4, Timestamp:              0, RTT:    1078
Index:  5, Timestamp:              0, RTT:    1114
Index:  6, Timestamp:              0, RTT:    1570
Index:  7, Timestamp:              0, RTT:    6865
Index:  8, Timestamp:              0, RTT:    1035
Index:  9, Timestamp:              0, RTT:    1334
Index: 10, Timestamp:              0, RTT:    1090
Index: 11, Timestamp:              0, RTT:    1099
Index: 12, Timestamp:              0, RTT:    1429
Index: 13, Timestamp:              0, RTT:    1048
Index: 14, Timestamp:              0, RTT:     985
Index: 15, Timestamp:              0, RTT:    1002
Index: 16, Timestamp:              0, RTT:    1013
Index: 17, Timestamp:              0, RTT:    1741
Index: 18, Timestamp:              0, RTT:    1231
Index: 19, Timestamp:              0, RTT:    1517
Index: 20, Timestamp:              0, RTT:    7780
Index: 21, Timestamp:              0, RTT:    1018
Index: 22, Timestamp:              0, RTT:    1036
Index: 23, Timestamp:              0, RTT:    2369
Index: 24, Timestamp:              0, RTT:    1120
Index: 25, Timestamp:              0, RTT:    1062
Index: 26, Timestamp:              0, RTT:    1088
Index: 27, Timestamp:              0, RTT:    1073
Index: 28, Timestamp:              0, RTT:    1060
Index: 29, Timestamp:              0, RTT:    1071
Index: 30, Timestamp:              0, RTT:    1116
Index: 31, Timestamp:              0, RTT:    1075
Index: 32, Timestamp:              0, RTT:    1084
```

Related Commands

Command	Description
policy-route	Configures policy based routing on an interface.

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.3(1)	This command was added.
8.4(1)	Show password encryption in user context was added.

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:

```
ciscoasa# 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.

Command Default

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Support for this command was added 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.

Note ASA takes time to calculate and display the Current and Average counters with accurate values. The default value for the Perfmon Stat Refresh interval for the Current value is 120 seconds. The Average counter is calculated based on the average of the values from the last time **clear perfmon** was executed or when the command was not used, from the time the device was started.

Examples

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

```
ciscoasa(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:

```
ciscoasa(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 (Deprecated)

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(4)	This command was added.
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.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Examples

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

```
ciscoasa
(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
ciscoasa
(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:

```
ciscoasa
(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
ciscoasa
(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:

```
ciscoasa
(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 bsr-router

To display the bootstrap router (BSR) information, use the show pim bsr-router command

show pim bsr-router

Syntax Description

No arguments or variables.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.5(2)	This command was added.

Examples

The following is sample output from the **show pim bsr-router** command:

```
ciscoasa# show pim bsr-router
PIMv2 Bootstrap information
This system is a candidate BSR
  Candidate BSR interface GigabitEthernet0/0 is down - BSR messages not originated
  Candidate RP: 4.4.4.1(GigabitEthernet0/0), GigabitEthernet0/0 is down - not advertised
```

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command also displays the winner metric towards the RP.

Examples

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

```
ciscoasa# 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 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.
rp-timers	(Optional) Displays uptime and expiry timers of group-to-RP mapping.

Command Default

Displays group-to-protocol mappings for all groups.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was modified to include the rp-timers variable.

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. To see the elected RP for a group, specify the group address or name in the **show pim group-map** command.

Examples

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

```
ciscoasa# 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.

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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.

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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.

Command Default

Topology information for all groups and sources is shown.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

```
ciscoasa# 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.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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.

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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 policy-list

To display information about a configured policy list and policy list entries, use the **show policy-list** command in user EXEC or privileged EXEC mode.

show policy-list [*policy_list_name*]

Syntax Description

policy_list_name	(Optional) Display information about the specified policy list.

Command Default

If you do not specify a policy list name, this command shows all of the policy lists.

Command Modes

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

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

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Policy lists are used in BGP routing as matching criteria for route maps.

Examples

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

```
ciscoasa# show policy-list

policy-list policy_list_2 permit
  Match clauses:
    ip address prefix-lists: prefix_1
policy-list policy_list_1 permit
  Match clauses:
    ip address (access-lists): test
    interface inside
```

Related Commands

Command	Description
policy-list	Configures policy lists.

show policy-route

To display the policy-based routing configuration, use the **show policy-route** command in user EXEC or privileged EXEC mode.

show policy-route

Command Modes

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

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

Command History

Release	Modification
9.4(1)	This command was added.

Examples

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

```
ciscoasa# show policy-route

Interface            Route map
GigabitEthernet0/0   equal-access
```

Related Commands

Command	Description
policy-route	Configures policy-based routing.

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:

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

Command History

Release	Modification
8.4(1)	This command was added.

Examples

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

```
ciscoasa# 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:

```
ciscoasa# 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:

```
ciscoasa# 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:

```
ciscoasa# 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:

```
ciscoasa# 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.
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 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:

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

Command History

Release	Modification
8.4(1)	This command was added.

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:

```
ciscoasa# 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):

```
ciscoasa# 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:

```
ciscoasa# 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 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 power inline

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

show power inline

Note Supported for the Firepower 1010 and ASA 5505 only.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Added support for the Firepower 1010.

Usage Guidelines

You can use PoE interfaces to connect devices that require power, such as an IP phone or a wireless access point. For the Firepower 1010, Ethernet 1/7 and 1/8 support PoE+. For the ASA 5505, Ethernet 0/6 and 0/7 support PoE.

Examples

The following is sample output from the **show power inline** command for the Firepower 1010:

```
ciscoasa# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

The following is sample output from the **show power inline** command for the ASA 5505:

```
ciscoasa# 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 11-1 shows each field description:

Table 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	(ASA 5505) 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.
Class	(Firepower 1010) Shows the PoE class of the connected device.
Current (mA)	(Firepower 1010) Shows the current being used.
Voltage (V)	(Firepower 1010) Shows the voltage being used.

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.
power inline	Enables or disables PoE.
show interface	Displays the runtime status and statistics of interfaces.

show prefix-list

To display information about configured prefix lists, use the **show prefix-list** command in user EXEC or privileged EXEC mode.

show prefix-list [**summary | detail**] [*policy_list_name* [**seq** *sequence_number* | *network/length* [**longer | first-match**]]]

Syntax Description

policy_list_name	(Optional) Display information about the specified policy list.
summary	(Optional) Show additional summarized statistical information.
detail	(Optional) Show additional summarized statistical information plus prefix list entries.
seq *sequence_number*	(Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix list.
network/length [**longer** | **first-match**]	(Optional) Displays all entries in the specified prefix list that use this network address and netmask length (in bits). The length of the network mask can be from 0 to 32. You can add these keywords to modify the match: • **longer**—Displays all entries of the specified prefix list that match or are more specific than the given network/length. • **first-match**—Displays the first entry of the specified prefix list that matches the given network/length.

Command Default

If you do not specify a prefix list name, this command shows all of the prefix lists. If you do not include other keywords, the output shows the prefix list entries only.

Command Modes

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

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

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Prefix lists are used in routing as matching criteria for route maps and policy lists.

Examples

The following is sample output from the **show prefix-list** command.

```
ciscoasa# show prefix-list

prefix-list prefix_1: 1 entries
   seq 1 permit 2.0.0.0/8
```

The following is an example of summarized output.

```
ciscoasa# show prefix-list summary

Prefix-list with the last deletion/insertion: prefix_1
prefix-list prefix_1:   Description: FirstPrefixList
   count: 1, range entries: 0, sequences: 1 - 1, refcount: 3
```

The following is an example of detailed output.

```
ciscoasa# show prefix-list detail

Prefix-list with the last deletion/insertion: prefix_1
prefix-list prefix_1:   Description: FirstPrefixList
   count: 1, range entries: 0, sequences: 1 - 1, refcount: 3
   seq 1 permit 2.0.0.0/8 (hit count: 0, refcount: 1)
```

Related Commands

Command	Description
prefix-list	Configures prefix lists.

show priority-queue

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

show priority-queue { **config | statistics** } [*interface_name*]

Syntax Description

config	Show the queue and TX-ring limits for the interface priority queues.
interface_name	(Optional) Specifies the name of the interface for which you want to show the configuration or the best-effort and low-latency queue statistical details.
statistics	Show the best-effort and low-latency queue statistical details.

Command Default

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

This example shows statistics for the interface named test. In the output, BE indicates the best-effort queue, and LLQ represents the low-latency queue:

```
ciscoasa# 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
ciscoasa#
```

The following example shows the configuration of the priority queues on all configured interfaces.

```
ciscoasa# show priority-queue config

Priority-Queue Config interface inside
               current         default         range
queue-limit    0               2048            0 - 2048
tx-ring-limit  4294967295              511             3 - 511
Priority-Queue Config interface test
               current         default         range
queue-limit    0               2048            0 - 2048
tx-ring-limit  4294967295              511             3 - 511
Priority-Queue Config interface outside
               current         default         range
queue-limit    0               2048            0 - 2048
tx-ring-limit  4294967295              511             3 - 511
Priority-Queue Config interface bgmember1
               current         default         range
queue-limit    0               2048            0 - 2048
tx-ring-limit  4294967295              511             3 - 511
ciscoasa#
```

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.
priority-queue	Configures priority queuing 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 details for each process.
non-zero	(Optional) Shows processes with non-zero CPU usage.
sorted	(Optional) Shows sorted CPU usage for processes.

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.
7.0(4)	The runtime value was enhanced to display accuracy within one millisecond.
7.2(1)	The output was enhanced to display more detailed information about processes that hog the CPU.
8.0(1)	Added the cpu-usage keyword.
9.2(1)	The output was enhanced to display CPU hog detection information.

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.
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.

The ASA runs as a single process with many different threads of execution. The output of this command actually shows memory allocations and free memory on a per-thread basis. Because these threads work in cooperation on data flows and other operations pertinent to operation of the ASA, one thread may allocate a block of memory while a different thread may free it. The last row of output contains the total counts over all threads. Only this row may be used to track potential memory leaks by monitoring the difference between allocations and free memory.

Examples

The following example shows how to list processes with non-zero CPU usage. In this example, the ASA 5555 platform uses two DATAPATH threads for packet processing and several control plane processes. The output consolidates the information. The nomenclature for DATAPATH threads are <thread-name>-<core-id>-<process-id> So we know that from output of show process, there are two data path threads running on logical core 0 and 1 with process id 2332 and 2333. If these percentages are high, consider ways to alleviate the load on the machine. For example, if you are running VPN, consider split tunneling or VPN load balancing.

```
ciscoasa# sh processes cpu-usage non-zero
Hardware:   ASA5555
Cisco Adaptive Security Appliance Software Version 9.9(2)56
ASLR enabled, text region 7f83f20fe000-7f83f65ea5cc
PC                  Thread                5Sec     1Min     5Min   Process
0x00007f83f49338b5  0x00002aaac9ead080     0.0%     0.2%     0.2%   vpnfol_thread_timer
0x00007f83f4722e18  0x00002aaac9eddbe0     0.1%     0.0%     0.0%   UserFromCert Thread
0x00007f83f4722e18  0x00002aaac9eae9e0     0.7%     0.4%     0.4%   Unicorn Proxy Thread
0x00007f83f465b6ec  0x00002aaac9ece1c0     0.4%     0.4%     0.4%   Logger
0x00007f83f4272a53  0x00002aaac9ec3b00     0.1%     0.1%     0.1%   Crypto CA
0x00007f83f2f97df9  0x00002aaac9ebcaa0     0.2%     0.2%     0.2%   CP Processing
0x00007f83f52277ed  0x00002aaac9ed1480     0.0%     0.1%     0.0%   Checkheaps
0x00007f83f42c8c83  0x00002aaac9ec3760     0.1%     0.0%     0.0%   CERT API
0x00007f83f347b722  0x00002aaac9eb7740     0.1%     0.1%     0.1%   ARP Thread
                  -                 -       37.1%    36.8%    36.3%   DATAPATH-0-2332
                  -                 -       37.2%    36.8%    36.3%   DATAPATH-1-2333
```

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

```
ciscoasa#  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:

```
ciscoasa# 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 examples show how to display the number and detail of processes that are hogging the CPU:

```
ciscoasa# show processes cpu-hog
 Granular CPU hog detection currently running, started at 15:41:16 UTC Jan 6 2014.
 Sample count: 10000 Threshold: 10ms
 Granular CPU hog detection completed at 15:41:16 UTC Jan 6 2014.
 Sample count: 10000 Threshold: 10ms
 The remainder of the CPU hog traceback follows:
 Process: DATAPATH-0-2042, NUMHOG: 430, MAXHOG: 22, LASTHOG: 2
 LASTHOG At: 15:42:21 UTC Jan 6 2014
 PC: 0x0000000000000000 (suspend)
 Call stack: 0x000000000041c98c 0x000000000041cc99 0x000000000069b0f0
```

```
0x00000000013619af 0x000000000136cbbd 0x0000000001372203
0x00007ffffeab2f3a
Interrupt based hog #1
Hog #1, traceback #1, at: 15:41:16 UTC Jan 6 2014, hog 20 ms
PC: 0x0000000000eb616b
Call stack: 0x0000000001360281 0x00007ffffeaba5f0 0x0000000000ebcf71
0x0000000000ebc5ab 0x0000000000ebcb0e 0x0000000000e17410
0x0000000000e19ac4 0x0000000000e19e55 0x0000000000ca50b4
0x0000000001344419 0x000000000069b315 0x000000000069be9e
0x000000000069b0a4 0x00000000013619af
Hog #1, traceback #2, at: 15:41:16 UTC Jan 6 2014, hog 21 ms
PC: 0x0000000000e8fc41
Call stack: 0x0000000001360281 0x00007ffffeaba5f0 0x0000000000e17410
0x0000000000e19ac4 0x0000000000e19e55 0x0000000000ca50b4
0x0000000001344419 0x000000000069b315 0x000000000069be9e
0x000000000069b0a4 0x00000000013619af 0x000000000136cbbd
0x0000000001372203 0x00007ffffeab2f3a
Interrupt based hog #2
Hog #2, traceback #1, at: 15:41:36 UTC Jan 6 2014, hog 9 ms
PC: 0x0000000000eb6167
Call stack: 0x0000000001360281 0x00007ffffeaba5f0 0x0000000000ebcf71
0x0000000000ebc5ab 0x0000000000ebcb0e 0x0000000000e17410
0x0000000000e19ac4 0x0000000000e19e55 0x0000000000ca50b4
0x0000000001344419 0x000000000069b315 0x000000000069be9e
0x000000000069b0a4 0x00000000013619af
Interrupt based hog #3
Hog #3, traceback #1, at: 15:42:21 UTC Jan 6 2014, hog 2 ms
PC: 0x000000000068a223
Call stack: 0x0000000001360281 0x00007ffffeaba5f0 0x000000000069bbba
0x000000000069b0a4 0x00000000013619af 0x000000000136cbbd
0x0000000001372203 0x00007ffffeab2f3a
```

The following example shows the memory allocation for each process:

```
ciscoasa# 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
```

Where,

- Allocs—Number of times memory was allocated for the process from the system startup time.
- Allocated—Total memory allocated for the process from the system startup time.
- Frees—Number of times free memory was requested for the process from the system startup time.
- Freed—Total memory released by the process from the system startup time.

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

```
ciscoasa# 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)
```

Related Commands

Command	Description
show cpu	Shows the CPU usage information.

show ptp

To display a variety of PTP statistics and clock-related information, use the **show ptp** command in privileged EXEC or global configuration mode.

show ptp { **clock | internal-info | port** [*interface-name*] }

Note This command applies only to the Cisco ISA 3000 appliance.

Syntax Description

clock	Displays PTP clock properties.
internal-info	Displays PTP internal information, including port-specific counters.
port	Displays PTP port information for all PTP-enabled interfaces.
interface-name	Shows PTP port information for the specified interface.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

If you include the optional interface ID in the **show ptp port** command, the port information for only that interface is shown.

The **show ptp clock | port | internal-info** commands are also available in global configuration mode.

Examples

The following example shows PTP clock properties:

```
ciscoasa# show ptp clock
PTP CLOCK INFO
  PTP Device Type: Transparent Clock
  Operation mode: One Step
  Clock Identity: 0:8:2F:FF:FE:E8:43:81
  Clock Domain: 0
  Number of PTP ports: 4
```

The following example shows PTP port information for all PTP-enabled interfaces:

```
ciscoasa# show ptp port
PTP PORT DATASET: GigabitEthernet1/1
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 1
  PTP version: 2
  Port state: Enabled
PTP PORT DATASET: GigabitEthernet1/2
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 2
  PTP version: 2
  Port state: Disabled
PTP PORT DATASET: GigabitEthernet1/3
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 3
  PTP version: 2
  Port state: Disabled
PTP PORT DATASET: GigabitEthernet1/4
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 4
  PTP version: 2
  Port state: Enabled
```

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 [**ssh | telnet | http | username** *user*]

Syntax Description

ssh	Shows SSH sessions.
telnet	Shows Telnet sessions.
http	Shows HTTP sessions.
username *user*	Shows sessions for a given user.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.1(2)	This command was added.
9.12(1)	This command is now only available within a context, because the **quota management-session** command now supports quotas per context. Added the **ssh**, **telnet**, **http**, and **username** keywords. The display output now shows the number of sessions per protocol.

Usage Guidelines

This command shows the active administrative sessions by type.

Examples

The following example shows statistics for the current management session:

```
ciscoasa# show quota management-session
#Sessions               ConnectionType                 Username
1                              SSH                     cisco
2                              TELNET                  cisco
1                              SSH                     cisco1
```

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 raid

To display information about RAID status for the hard drives in the system, use the **show raid** command in privileged EXEC mode.

show raid

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.1(1)	This command was added.
9.17(1)	Support for the Secure Firewall 3100 was added.

Usage Guidelines

Some hardware models support two internal hard drives. For example, the ASA 5545-X and 5555-X support up to two solid state drives. When two drives are present, they are automatically formatted in a RAID-1 configuration. This structure is rebuilt every time you reload the device. You can use the **show raid** command to view information about the RAID configuration.

Note If a device model does not support RAID, you might get an invalid command error message when you enter the **show raid** command.

Examples

The following sample display shows two SSDs in the RAID on the Secure Firewall 3100:

```
> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
```

```
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

The following sample display shows one SSD in the RAID; disk2 is not present, and the RAID is shown as "degraded:"

```
> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

The following example for an ASA device shows that there is one active, working hard drive device, as shown by the State, Active Devices, and Working Devices lines. The output also shows that the second device is “removed,” as shown in the final table. This means either that no second drive was installed, or that the second drive has actually been removed.

```
ciscoasa# show raid
```

```
/dev/md0:
        Version : 1.2
  Creation Time : Mon Mar  6 09:04:14 2017
     Raid Level : raid1
     Array Size : 124969216 (119.18 GiB 127.97 GB)
  Used Dev Size : 124969216 (119.18 GiB 127.97 GB)
   Raid Devices : 2
  Total Devices : 1
    Persistence : Superblock is persistent
  Intent Bitmap : Internal
    Update Time : Tue Mar 21 14:03:27 2017
          State : active, degraded
 Active Devices : 1
Working Devices : 1
 Failed Devices : 0
  Spare Devices : 0
           Name : ciscoasa:0  (local to host ciscoasa)
           UUID : e8f90a6b:20433f38:e8b86378:6fd52057
         Events : 454610
    Number   Major   Minor   RaidDevice State
       0       8        0        0      active sync   /dev/sda
       1       0        0        1      removed
```

The following table explains the fields in the output.

Field	Description
Identifier	The array component identifier; for example, /dev/md0.
Version	The format of the Superblock (RAID metadata).
Creation Time	The date and time when this component was configured.
Raid Level	The raid level. RAID1 is a mirroring scheme.
Array Size	The total storage space available across all component devices in bytes (as well as gibibytes and gigabytes).
Used Dev Size	The amount of storage space contributed to the total by each device in bytes (as well as gibibytes and gigabytes). This is determined by the smallest device or partition; there may be unused space on larger devices.
RAID Devices	The total number of member devices in the complete array, including spare, missing, and failed devices.
Total Devices	The number of functional devices available.
Persistence	A persistent Superblock (the default when an array is created) means the Superblock is written to a specific location in all component devices of the array. The RAID configuration can then be read directly from the disks involved.
Update Time	The time at which the array status changed. Status changes include activation, failure, etc.

Field	Description
State	The current status of RAID. The first status indicates **active** if the array is fully operational, or **clean** if the array is active but there are no pending write operations. The possible statuses are: • active, resyncing—The system is new and it is currently building the RAID structure. It can take over 90 minutes to build the required structure. Look for a Rebuild Status line in the output, which indicates the percentage completed. • (clean or active), degraded, recovering—The RAID structure has been built successfully. • (clean or active), degraded—One hard drive is not functioning. It is either broken or missing. If you intend to have two drives, replace the broken or missing drive. • (clean or active), degraded, recovering—The system is in the process of rebuilding the RAID structure after installing or replacing a hard drive.
Active Devices	The number of currently functioning devices in the array; does not include spare devices.
Working Devices	The total number of operational (non-failed) devices in the array; that is, active devices plus spare devices.
Failed Devices	The number of failed devices in the array.
Spare Devices	The number of spare devices currently assigned to the array. If the array is missing a member, an available spare should get built into the array as an active member. But a drive can also be marked spare if the system failed to add it to the array.
UUID	The 128-bit hexadecimal universally unique identifier (UUID) stored in the array's Superblock. This number is randomly generated and used to uniquely tag a RAID. All component devices share this ID.
Events	Event counter for the array; incremented whenever the Superblock is updated.
Component table.	Component disks are numbered from 0. The Major number usually corresponds to the device type, while the Minor number is the identifier for a specific device in that group. For example, Major 8 indicates a SCSI disk. Each component of the RAID device is listed here, with the components current status. A healthy disk is in the **active sync** state.

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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:

```
ciscoasa# 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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
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.

```
ciscoasa# 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 11-2 shows each field description.

Table 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.

Examples

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

```
ciscoasa# 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
                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 11-3 shows each field description.

Table 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.

Command	Description
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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
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:

```
ciscoasa# 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-address es** —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.

Command Default

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	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
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:

```
ciscoasa# 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.

```
ciscoasa# 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:

```
ciscoasa# 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:

```
ciscoasa# 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 rest-api agent

To determine if the REST API Agent is currently enabled, use the **show rest-api agent** command in privileged EXEC mode.

show rest-api agent

Note This command is supported on all versions of ASA virtual, the ASA 5585-X, and all ASA 5500-X series devices except the ASA 5506-X and ASA 5508-X.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

Use this command to determine if the REST API Agent is currently enabled.

Examples

This example indicates that the REST API Agent is enabled:

```
ciscoasa(config)# show rest-api agent
REST API agent is currently enabled.
```

If the Agent is disabled, the message displayed is “REST API agent is currently disabled.”

Related Commands

Commands	Description
rest-api	Verify and install the REST API package. Enable the REST API Agent.
show version	If the REST API Agent is enabled, its version number is included in **show version** output.

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

```
ciscoasa# 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 rollback-status

When Cisco Security Manager sends a rollback request to ASA, the management connection from Cisco Security Manager to ASA is reset; the result of the rollback job cannot be sent to Cisco Security Manager. Use **show rollback-status** to display the status of rollback job to Cisco Security Manager when it queries ASA.

show rollback-status [*context_name*]

Syntax Description

context_name	The name of the context for which the rollback job is applied to. For single mode, this is not applicable.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.6(3)	This command was introduced.

Usage Guidelines

Use **show rollback-status** to display the status of rollback job, start, end time and context name the rollback job applied to.

Examples

The following examples show the rollback status for all contexts, entered in single mode:

1. Before any rollback request is received from Cisco Security Manager:

```
ciscoasa(config)# sh rollback-status
Status      : None
Start Time  : N/A
End Time    : N/A
```

2. When first rollback request is received on ASA, before the job is completed:

```
ciscoasa(config)# sh rollback-status
Status      : In Progress
Start Time  : 13:00:12 UTC May 11 2017
End Time    : N/A
```

3. When the rollback job is completed:

```
ciscoasa(config)# sh rollback-status
```

```
Status      : Succeeded
Start Time  : 13:00:12 UTC May 11 2017
End Time    : 13:00:14 UTC May 11 2017
```

4. If the rollback failed, its output would be:

```
ciscoasa(cfg-cluster)# sh rollback-status
Status      : Failed
Start Time  : 13:25:49 UTC May 11 2017
End Time    : 13:25:55 UTC May 11 2017
```

5. If the rollback failed, and it reverts to the startup config:

```
ciscoasa(cfg-cluster)# sh rollback-status
Status      : Reverted ( Roll back failed, startup config applied )
Start Time  : 13:25:49 UTC May 11 2017
End Time    : 13:25:55 UTC May 11 2017
```

The following examples show the rollback status entered in multiple mode and from system/admin context:

1. Before any rollback deployed into ASA:

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: admin
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

2. When the rollback on system context started:

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : In Progress
Start Time  : 16:55:35 UTC May 11 2017
End Time    : N/A
Context Name: admin
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

3. When the Rollback on system context is completed:

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : Succeeded
Start Time  : 19:52:25 UTC May 11 2017
End Time    : 19:52:34 UTC May 11 2017
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

4. When context name is specified in the command:

```
ciscoasa(config)# sh rollback-status system
Context Name: system
Status      : Succeeded
Start Time  : 19:52:25 UTC May 11 2017
End Time    : 19:52:34 UTC May 11 2017
ciscoasa(config)# sh rollback-status admin
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

The following examples show the rollback status entered in multiple mode and from admin/user context:

1. When no context name is specified:

```
ciscoasa/admin(config)# sh rollback-status
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

2. When context name is specified:

```
ciscoasa/admin(config)# sh rollback-status admin
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

3. When incorrect context name is specified

```
ciscoasa/admin(config)# sh rollback-status ad
Context ad does not exist.
```

4. When the context name does not match current context:

```
ciscoasa/admin(config)# sh rollback-status ctx1
Context ctx1 does not match current context.
```

When ASA is running as Slave or Standby unit, a warning message is displayed.

1. When the show command is issued from Slave, the output would be:

```
ciscoasa(config)# sh rollback-status
WARNING: Current unit is Slave.
```

2. When the show command issued from standby, the output would be:

```
ciscoasa(config)# sh rollback-status
WARNING: Current unit is Standby.
```

The following table describes the output entries in detail.

Output	Description
Context Name	The name of the context for which the rollback job is applied to. For single mode, this is not displayed.
Status	The status of the most recent rollback job. It can be any one of the following: • None—No rollback job has been ever deployed to this context. • In Progress—ASA has received the rollback request from Cisco Security Manager, and the rollback job is in progress. • Succeeded—The rollback has completed successfully. • Reverted—Rollback to the configure sent from Cisco Security Manager failed, rollback to the startup configure saved on the ASAis triggered, and this revert action is completed successfully, and now ASA is running the startup config. • Failed—Rollback completed with error.
Start Time	The start time for most recent rollback job. Whenever a rollback job is received on ASA, this field is updated with the current time on ASA; the Status is updated as “In Progress”. If rollback is in None state, “N/A” is displayed.
End Time	The time when rollback job is completed. If the job is completed without error, the “Status” is updated as “Succeeded”. If revert action has been taken during rollback, and revert is completed successfully, the status is updated as “Reverted”. If revert failed, the status is updated as “Failed”. For rollback in “None” or “In Progress” state, “N/A” is displayed.

show route

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

The parameters you can use with this command differ depending on the firewall mode of the device, routed or transparent. This is indicated in the syntax description.

show route [**management-only** [*interface_name*]] [**cluster | failover |** *hostname* | *ip_address* [*mask*] [**longer-prefixes**] | **domain-name** *hostname_or_ip_address* | **bgp** [*as_number*] **| connected | eigrp** [*process_id*] **| isis | isis | ospf** [*process_id*] **| rip | static | summary | zone**]

Syntax Description

bgp *as_number*	(Routed.) Displays the routing information base (RIB) epoch number (sequence number), the current timer value, and the network descriptor block epoch number (sequence number) for the BGP route. The *as_number* limits the display to route entries that use the specified AS number.
cluster	(Routed.) Displays the routing information base (RIB) epoch number (sequence number), the current timer value, and the network descriptor block epoch number (sequence number).
connected	(Routed, transparent.) Displays connected routes.
domain-name *hostname_or_ip_address*	(Routed, transparent.) Displays routes to the specified destination hostname. You must configure DNS for hostname resolution to work. You can also use an IP address on this keyword.
eigrp *process_id*	(Routed.) Displays EIGRP routes.
failover	(Routed.) Displays the current sequence number of the routing table and routing entries after failover has occurred, and a standby unit becomes the active unit.
hostname	(Routed, transparent.) Displays routes to the specified destination hostname. You must configure DNS for hostname resolution to work.
interface_name	(Routed, transparent.) Displays route entries that use the specified interface.
ip_address mask	(Routed, transparent.) Displays routes to the specified destination.
isis	(Routed.) Displays IS-IS routes.
longer-prefixes	(Routed, transparent.) Displays routes that match the specified *ip_address* /*mask* pair only
management-only	(Routed, transparent.) Displays routes in the IPv4 management routing table.
isis	(Routed.) Displays IS-IS routes.
ospf *process_id*	(Routed.) Displays OSPF routes.
rip	(Routed.) Displays RIP routes.
static	(Routed, transparent.) Displays static routes.

summary	(Routed, transparent.) Displays the current state of the routing table.
zone	(Routed, transparent.) Displays the routes for zone interfaces.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The **eigrp** keyword was added.
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.
9.2(1)	The **bgp** keyword was added.
9.2(1)	The command now displays the local host routes, along with **connected** routes. New codes (L, I, E, su and +) are added to indicate the protocol or type of route being displayed.
9.3(2)	The **zone** keyword was added.
9.5(1)	Support for the management routing table feature was added.
9.6(1)	We added the **isis** keyword.
9.6(1)	The **isis** keyword was added.
9.20(2)	The **domain-name** keyword was added.

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.

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.

Examples

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

```
ciscoasa# show route
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, 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, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated 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 5555, in the admin context. The output displays the internal loopback address, which is used by the VPN hardware client for individual user authentication.

```
ciscoasa/admin(config)# show route
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, 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, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated 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 from the **show route bgp** command:

```
ciscoasa# show route bgp
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route
Gateway of last resort is 10.86.116.1 to network 0.0.0.0
```

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:

```
ciscoasa(config)# show route failover
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, 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, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated 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:

```
ciscoasa(cfg-cluster)# show route cluster
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, 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, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated 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
```

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

```
ciscoasa# show route summary
IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          1           0           0           88          288
bgp 2           0           0           0           0           0
  External: 0 Internal: 0 Local: 0
internal        1                                               408
Total           2           2           0           264         1272
```

See the following output for the **show route zone** command:

```
ciscoasa# show route zone
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
S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

The following example shows output from the **show route isis** command.

```
ciscoasa# show route isis
Routing Table:
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route
Gateway of last resort is not set
i L2     1.1.1.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     2.2.2.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     3.3.3.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     4.4.4.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     5.5.5.0 255.255.255.0 [115/10] via 22.22.22.5, subint
```

show running-config

To display the configuration that is currently running on the ASA, use the **show running-config** command in privileged EXEC mode.

show running-config [**all**] [*command*]

Syntax Description

all	Displays the entire operating configuration, including defaults.
command	Displays the configuration associated with a specific command. For available commands, see the CLI help using **show running-config ?**.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.3(1)	Encrypted passwords were added to the output.
9.7(1)	The output from this command will also display syslog servers configured with IPv6 addresses.
9.13(1)	• The telemetry configuration details were included in the output. • New command—**tftp blocksize** was added to display the configured blocksize value except the default value.

Usage Guidelines

The show running-config command displays the active configuration in memory (including saved configuration changes) on the ASA.

To display the saved configuration in flash memory on the ASA, use the **show configuration** command.

The **show running-config** command output displays encrypted, masked, or clear text passwords when password encryption is either enabled or disabled.

Note ASDM commands appear in the configuration after you use it to connect to or configure the ASA.

The default for **error-recovery disable** changed to disabled in ASA release 9.3. For that reason, you may notice that the **show running-config** command now shows *error-recovery disable* in the CLI when WebVPN error recovery is at the default value. We recommend to leave it disabled unless advised by Cisco's Technical Assistance Center while troubleshooting a problem.

From ASA 9.13(1), the telemetry details were included to the output of this command. The show running-config command shows only the non-default configuration (**no service telemetry**) of the telemetry service. Use the **all** command to also view the default telemetry service configuration.

Examples

The following is sample output from the **show running-config** command:

```
ciscoasa# show running-config
: Saved
:
ASA Version 9.0(1)
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.1.1.2 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.3 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname example1
domain-name example.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
```

```
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.1.1.2
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map abc_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy abc_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

The following is sample output from the **show running-config access-group** command:

```
ciscoasa# show running-config access-group
access-group 100 in interface outside
```

The following is sample output from the **show running-config arp** command:

```
ciscoasa# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

To view the BFD global configuration settings, use output modifiers to filter the BFD related configuration. The following is sample output from the **show running-config bfd** command using the output modifiers:

```
ciscoasa# show running-config bfd
bfd map ipv4 1.1.1.1/24 1.1.1.2/32 name2
```

The following is sample output from the **show running-config bfd-template** command using the output modifiers:

```
ciscoasa# show running-config bfd-template
bfd-template single-hop bfd_template
interval min-tx 50 min-rx 50 multiplier 3
!
bfd-template single-hop bfd_template_auth
interval min-tx 50 min-rx 50 multiplier 3
authentication md5 ***** key-id 8
!
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
show configuration	Shows the startup configuration.