show is - show m

show isakmp ipsec-over-tcp stats

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

show isakmp ipsec-over-tcp stats

Syntax Description

This command has no arguments or keywords.

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	• Yes	—
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
ASA virtual(1)	The **show isakmp ipsec-over-tcp stats** command was added.
7.2(1)	The **show isakmp ipsec-over-tcp stats** command was deprecated. The **show crypto isakmp ipsec-over-tcp stats** command replaced it.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The output from this command includes the following fields:

- Embryonic connections
- Active connections
- Previous connections
- Inbound packets
- Inbound dropped packets
- Outbound packets
- Outbound dropped packets
- RST packets

- Received ACK heart-beat packets
- Bad headers
- Bad trailers
- Timer failures
- Checksum errors
- Internal errors

Examples

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

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

Related Commands

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

show isakmp sa

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

show isakmp sa [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

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	• Yes	—
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The **show isakmp sa** command was added.
7.2(1)	This command was deprecated. The **show crypto isakmp sa** command replaced it.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The output from this command includes the following fields:

Detail not specified.

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

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

Examples

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

```
ciscoasa(config)# show isakmp sa detail
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
ciscoasa(config)#
```

Related Commands

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

show isakmp stats

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

show isakmp stats

Syntax Description

This command has no arguments or keywords.

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	• Yes	—
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
ASA virtual(1)	The **show isakmp stats** command was added.
7.2(1)	This command was deprecated. The **show crypto isakmp stats** command replaced it.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

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

- Active/Standby Tunnels—cikePhase1GWActiveTunnels
- Previous Tunnels—cikePhase1GWPreviousTunnels
- In Octets—cikePhase1GWInOctets
- In Packets—cikePhase1GWInPkts
- In Drop Packets—cikePhase1GWInDropPkts
- In Notifys—cikePhase1GWInNotifys
- In P2 Exchanges—cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids—cikePhase1GWInP2ExchgInvalids

- In P2 Exchange Rejects—cikePhase1GWInP2ExchgRejects
- In P2 Sa Delete Requests—cikePhase1GWInP2SaDelRequests
- Out Octets—cikePhase1GWOutOctets
- Out Packets—cikePhase1GWOutPkts
- Out Drop Packets—cikePhase1GWOutDropPkts
- Out Notifys—cikePhase1GWOutNotifys
- Out P2 Exchanges—cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids—cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects—cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests—cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels—cikePhase1GWInitTunnels
- Initiator Fails—cikePhase1GWInitTunnelFails
- Responder Fails—cikePhase1GWRespTunnelFails
- System Capacity Fails—cikePhase1GWSysCapFails
- Auth Fails—cikePhase1GWAuthFails
- Decrypt Fails—cikePhase1GWDecryptFails
- Hash Valid Fails—cikePhase1GWHashValidFails
- No Sa Fails—cikePhase1GWNoSaFails

The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets

- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

Examples

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

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

Related Commands

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

show isis database

To display the IS-IS link-state database, use the **show isis database** command in privileged EXEC mode.

show isis database [{ **detail | verbose** }[**ip** [**unicast**] **| ipv6** [**unicast**]][**topology base**]][**level-1 | level-2**]

Syntax Description

level-1	(Optional) Displays the IS-IS link-state database for Level 1.
level-2	(Optional) Displays the IS-IS link-state database for Level 2.
ip	(Optional) Shows the IS-IS link-state database for the IPv4 address-family
ipv6	(Optional) Shows the IS-IS link-state database for the IPv6 address-family
detail	(Optional) Displays the contents of each link-state packet (LSP).
verbose	(Optional) Displays additional information about the Intermediate IS-IS database.
topology base	(Optional) Shows the MTR topology.
unicast	(Optional) Shows unicast address families.

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
9.6(1)	We introduced this command.

Usage Guidelines

This command displays the IS-IS link-state database.

Examples

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

```
ciscoasa# show isis database
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d300     0x3d0d              674                     0/0/0
```

```
routerA.00-00     0x1b541556     0xa349               928                       0/0/0
c3.00-00              0x9257c979     0x9952               759                       0/0/0
c2.00-00             *0xef11e977     0x3188               489                       0/0/0
c2.01-00             *0xa8333f03     0xd6ea               829                       0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f24      0xaba2               526                       0/0/0
routerA.00-00     0x0d540b55      0x81d7               472                       0/0/0
routerA.00-01     0xffffff01          0xe20b              677                       0/0/0
c3.00-00              0x002e5434      0xb20a              487                       0/0/0
c2.00-00             *0x74fd1227      0xbb0f              742                       0/0/0
c2.01-00             *0x7ee72c1a      0xb506              968                       0/0/0
```

Table 1: show isis database Fields

Field	Description
LSPID	The LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is nonzero, the LSP describes links from the system. When it is zero, the LSP is a so-called nonpseudonode LSP. This mechanism is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP will describe the state of the originating router. For each LAN, the designated router for that LAN will create and flood a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP will be divided into multiple LSP fragments. Each fragment will have a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP will stay in the LSDB before being completely removed.
ATT	The Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers will use the Attach bit to find the closest Level 2 router. They will point a default route to the closest Level 2 router.
P	The P bit. Detects if the intermediate systems is area partition repair-capable. Cisco and other vendors do not support area partition repair.
OL	The Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers will not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router will be sent to this router.

The following is sample output from the **show isis database detail** command. As the output shows, in addition to the information displayed with the **show isis database** command, the **show isis database detail** command displays the contents of each LSP.

```
ciscoasa# show isis database detail
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d301      0x3b0e              1189                     0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00      0x1b541556     0xa349               642                      0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

Table 2: show isis database detail Fields

Field	Description
Area Address	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system [ES], or a CLNS prefix).

The following is additional sample output from the **show isis database detail** command. This LSP is a Level 2 LSP. The area address 39.0001 is the address of the area in which the router resides.

```
ciscoasa# show isis database l2 detail
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f25      0xa9a3              1076                     0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IS c2.01
routerA.00-00      0x0d540b56     0x7fd8               941                      0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IS c2.01
  Metric:          0 IP-External 1.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.2.2.0 255.255.255.0
  Metric:          0 IP-External 3.1.1.0 255.255.255.0
```

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

```
ciscoasa# show isis database verbose
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00            *0xea19d301   0x3b0e        644               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   22.22.22.1
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00         0x1b541557   0xa14a        783               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   22.22.22.5
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

Table 3: show isis database verbose Fields

Field	Description
LSPID	Link-state packet (LSP) identifier. The first six octets form the System ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a pseudonode LSP. This is similar to a router LSA in Open Shortest Path First (OSPF); the LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP that describes all systems attached to that LAN. The last octet is the LSP number. If all the data cannot fit into a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the system issuing this command originated the LSP.
LSP Seq Num	LSP sequence number that allows other systems to determine if they received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time that the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from all routers' link-state databases (LSDBs). The value indicates how long the purged LSP will stay in the LSDB before it is completely removed.
ATT	Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1 routers use the Attach bit to find the closest Level 2 router. They install a default route to the closest Level 2 router.
P	P bit. This bit detects if the IS can repair area partitions. Cisco and other vendors do not support area partition repair.
OL	Overload bit. This bit determines if the IS is congested. If the overload bit is set, other routers do not use this system as a transit router when they calculate routes. Only packets for destinations directly connected to the overloaded router are sent to this router.

Field	Description
Area Address	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
NLPID	Network Layer Protocol identifier.
Hostname	Hostname of the node.
Router ID	Traffic engineering router identifier for the node.
IP Address	IPv4 address for the interface.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system (ES), or a Connectionless Network Service [CLNS] prefix).
Affinity	Link attribute flags that are being flooded.
Physical BW	Link bandwidth capacity (in bits per second).
Reservable BW	Amount of reservable bandwidth on this link.
BW Unreserved	Amount of bandwidth that is available for reservation.

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.

Command	Description
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.

Command	Description
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis hostname

To display the router-name-to-system-ID mapping table entries for an IS-IS router, use the **show isis hostname** command in privileged EXEC mode.

show isis hostname

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	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

In the IS-IS routing domain, the system ID is used to represent each router. The system ID is part of the network entity title (NET) that is configured for each IS-IS router. For example, a router with a configured NET of 49.0001.0023.0003.000a.00 has a system ID of 0023.0003.000a. Router-name-to-system-ID mapping is difficult for network administrators to remember during maintenance and troubleshooting on the routers. Entering the **show isis hostname** command displays the entries in the router-name-to-system-ID mapping table.

If the dynamic hostname feature has not been disabled by entering the **no hostname dynamic** command, the mapping will consist of a dynamic host mapping table.

Examples

The following example changes the hostname to ciscoASA and assigns the NET 49.0001.0050.0500.5005.00 to ciscoASA:

```
ciscoasa(config)# hostname ciscoASA
ciscoASA(config)# router isis
ciscoASA(config-router)# net 49.0001.0050.0500.5005.00
ciscoASA(config-router)# hostname dynamic
ciscoASA(config-router)#
```

Entering the **show isis hostname** command displays the dynamic host mapping table. The dynamic host mapping table displays the router-name-to-system-ID mapping table entries for ciscoASA, c2, c3 and for the local router named routerA. The table also shows that c3 is a Level-1 router, and its hostname is advertised by the Level-1 (L1) link-state protocol (LSP). C2 is a Level-2 router and its

hostname is advertised by the L2 LSP. The * symbol that appears under Level for the ASA ciscoASA signifies that this is the router-name-to-system-ID mapping information for the ASA.

```
ciscoASA# show isis hostname
Level  System ID       Dynamic Hostname  (c1)
     * 0050.0500.5005   ciscoASA
    1  0050.0500.5007   c3
    2  0050.0500.5006   routerA
    2  0050.0500.5008   c2
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).

Command	Description
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.

Command	Description
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis lsp-log

To display the Level 1 and Level 2 IS-IS link-state packet (LSP) log of the interfaces that triggered the new LSP, use the **show isis lsp-log** command in privileged EXEC mode.

show isis lsp-log

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	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

Displays the Level 1 and Level 2 IS-IS link-state packet (LSP) log of the interfaces that triggered the new LSP.

Examples

The following is sample output from the **show isis lsp-log** command:

```
ciscoasa# show isis lsp-log
    Level 1 LSP log
  When       Count       Interface         Triggers
  04:16:47     1         subint             CONFIG NEWADJ DIS
  03:52:42     2         subint             NEWADJ DIS
  03:52:12     1         subint             ATTACHFLAG
  03:31:41     1         subint             IPUP
  03:30:08     2         subint             CONFIG
  03:29:38     1         subint             DELADJ
  03:09:07     1         subint             DIS ES
  02:34:37     2         subint             NEWADJ
  02:34:07     1         subint             NEWADJ DIS
    Level 2 LSP log
  When       Count       Interface         Triggers
  03:09:27     1         subint             CONFIG NEWADJ
  03:09:22     1         subint             NEWADJ
  02:34:57     2         subint             DIS
  02:34:50     1                                IPUP
  02:34:27     1         subint             CONFIG DELADJ
  02:13:57     1         subint             DELADJ
  02:13:52     1         subint             NEWADJ
```

```
01:35:58     2         subint             IPIA
01:35:51     1                               AREASET IPIA
```

Table 4: show isis lsp-log Fields

Field	Description
When	Time elapsed since the LSP was generated.
Count	Number of events that took place at this time.
Interface	Interface that caused the LSP regeneration.
Triggers	Event that triggered the LSP to be flooded. Possible triggers for an LSP are as follows: • AREASET—Active area set changed. • ATTACHFLAG—Attach bit changed state. • CLEAR—Some form of manual clear command was issued. • CONFIG—Any configuration change. • DELADJ—Adjacency went down. • DIS—DIS changed or pseudonode changed. • ES—End System adjacency changed. • HIPPITY—LSPDB overload bit changed state. • IF_DOWN—Needs a new LSP. • IP_DEF_ORIG—Default information originate changed. • IPDOWN—Directly connected IP prefix down. • IP_EXTERNAL—Redistributed IP route appeared or gone. • IPIA—Interarea IP route appeared or gone. • IPUP—Directly connected IP prefix up. • NEWADJ—New adjacency came up. • REDIST—Redistributed level-2 CLNS route changed. • RRR_INFO—RRR bandwidth resource information.

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.

Command	Description
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.

Command	Description
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.

Command	Description
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis neighbors

To display information about IS-IS neighbors, use the **show isis neighbors** command in privileged EXEC mode.

show isis neighbors [**detail**]

Syntax Description

detail	(Optional) Displays more detailed information for IS-IS neighbors.

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
9.6(1)	We introduced this command.

Usage Guidelines

The **show isis neighbors** command is used to display brief information about connected IS-IS routers. Enter the **detail** keyword to display more detailed information.

Examples

The show **isis neighbors command** is entered to display information about the IS-IS neighbor routerA:

```
ciscoasa# show isis neighbors
System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint        22.22.22.5        UP    21             c2.01
routerA          L2    subint        22.22.22.5        UP    22             c2.01
c2                   L1    subint        22.22.22.3        UP     9              c2.01
c2                   L2    subint        22.22.22.3        UP     9              c2.01
```

The **show isis neighbors detail** command is entered to display more detailed information about the IS-IS neighbor routerA:

```
ciscoasa# show isis neighbors detail
System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint        22.22.22.5        UP    23             c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
```

```
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
routerA          L2    subint        22.22.22.5        UP    22             c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
```

Table 5: show isis neighbors Fields

Field	Description
System Id	Six-byte value that identifies a system in an area.
Type	Level type. Indicates whether the IS-IS neighbor is a Level 1, Level-1-2, or Level 2 router.
Interface	Interface from which the system was learned.
IP Address	IP address of the neighbor router.
State	Indicates whether the state of the IS-IS neighbor is up or down.
Holdtime	Link-state packet (LSP) holdtime. Amount of time that the LSP remains valid (in seconds).
Circuit Id	Port location for the IS-IS neighbor router that indicates how it is connected to the local router.
Area Address(es)	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
SNPA	Subnetwork point of attachment. This is the data-link address.
State Changed	State change.
LAN Priority	Priority of the LAN.
Remote TID	Neighbor router topology ID(s).
Local TID	Local router topology ID(s).

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.

Command	Description
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.

Command	Description
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.

Command	Description
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis rib

To display paths for a specific route or for all routes under a major network that are stored in the IP local Routing Information Base (RIB), use the **show isis rib** command in privileged EXEC mode.

show isis [***|** **ip** [**unicast**]] **|ipv6** [**unicast**]] **rib** [**redistribution** [**level-1 | level-2**]] [*network_ip* [*mask*]]

Syntax Description

*****	(Optional) Shows all IS-IS address families.
ip	(Optional) Shows the IPv4 address family.
ipv6	(Optional) Shows the IPv6 address family.
level-1	(Optional) Shows the Level 1 redistribution RIB.
level-2	(Optional) Shows the Level 2 redistribution RIB
network_ip [*mask*]	(Optional) Shows RIB information for a network.
redistribution	(Optional) Shows IS-IS IP redistribution RIB information
unicast	(Optional) Shows the unicast address family.

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
9.6(1)	We introduced this command.

Usage Guidelines

To verify that an IP prefix update that exists in the IP global RIB also has been updated in the IS-IS local RIB, enter the **show isis rib** command.

Examples

The following is sample output from the **show isis rib** command to show all routes that are stored within the IS-IS local RIB:

```
ciscoasa# show isis rib
IPv4 local RIB for IS-IS process
IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =
10.10.0.0 255.255.0.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]
10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]
10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

The following is sample output from the **show isis rib** command to show all routes under the major network 10.0.0.0 with the IP address 10.3.2.0 that are stored within the IS-IS local RIB:

```
ciscoasa# show isis rib 10.3.2.0
IPv4 local RIB for IS-IS process
IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =
Routes under majornet 10.0.0.0 255.0.0.0:
10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]
10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

The following is sample output from the **show isis rib** command to show all routes under the network with the IP address mask 10.3.2.0 255.255.255.0 that are stored within the IS-IS local RIB:

```
ciscoasa# show isis rib 10.3.2.0 255.255.255.0
IPv4 local RIB for IS-IS process
IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =
10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.

Command	Description
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.

Command	Description
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis spf-log

To display how often and why the router has run a full shortest path first (SPF) calculation, use the **show isis spf-log** command in privileged EXEC mode.

show isis [***| ip** [**unicast**] | **ipv6** [**unicast**]] **spf-log**

Syntax Description

*****	(Optional) Shows all IS-IS address families.
ip	(Optional) Shows the IPv4 address family.
ipv6	(Optional) Shows the IPv6 address family.
unicast	(Optional) Shows the unicast address family.

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 Modes

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

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

This command displays how often and why the router has run a full shortest path first (SPF) calculation.

Examples

The following is sample output from the **show isis ipv6 spf-log** command:

```
ciscoasa# show isis ipv6 spf-log
      TID 0 level 1 SPF log
  When   Duration  Nodes  Count     First trigger LSP   Triggers
00:15:46    3124     40      1          milles.00-00  TLVCODE
00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP
00:15:19    3096     41      1          deurze.00-00  TLVCODE
00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER
00:14:49    3384     41      1          milles.00-01  TLVCODE
00:14:23    2932     41      3          milles.00-00  TLVCODE
00:05:18    3140     41      1                        PERIODIC
00:03:54    3144     41      1          milles.01-00  TLVCODE
00:03:49    2908     41      1          milles.01-00  TLVCODE
00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT
```

```
00:03:15    3054     41      1          milles.00-00  TLVCODE
00:02:53    2958     41      1          mortel.00-00  TLVCODE
00:02:48    3632     41      2          milles.00-00  NEWADJ TLVCODE
00:02:23    2988     41      1          milles.00-01  TLVCODE
00:02:18    3016     41      1          gemert.00-00  TLVCODE
00:02:14    2932     41      1           bakel.00-00  TLVCONTENT
00:02:09    2988     41      2           bakel.00-00  TLVCONTENT
00:01:54    3228     41      1          milles.00-00  TLVCODE
00:01:38    3120     41      3            rips.03-00  TLVCONTENT
```

Table 6: show isis spf-log Fields

Field	Description
When	How long ago (in hours: minutes: seconds) a full SPF calculation occurred. The last 20 occurrences are logged.
Duration	Number of milliseconds required to complete this SPF run. Elapsed time is wall clock time, not CPU time.
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. A router waits 5 seconds before running a full SPF run, so it can include all new information. This count denotes the number of events (such as receiving new LSPs) that occurred while the router was waiting its 5 seconds before running full SPF.
First trigger LSP	Whenever a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue as to the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the last received LSP is remembered.
Triggers	A list of all reasons that triggered a full SPF calculation. See the next table for triggers.

Table 7: spf-log Triggers

Trigger	Description
ATTACHFLAG	This router is now attached to the Level 2 backbone or it has just lost contact to the Level 2 backbone.
ADMINDIST	Another administrative distance was configured for the IS-IS process on this router.
AREASET	Set of learned area addresses in this area changed.
BACKUPOVFL	An IP prefix disappeared. The router knows there is another way to reach that prefix but has not stored that backup route. The only way to find the alternative route is through a full SPF run.
DBCHANGED	A clear isis * command was issued on this router.

Trigger	Description
IPBACKUP	An IP route disappeared, which was not learned via IS-IS, but via another protocol with better administrative distance. IS-IS will run a full SPF to install an IS-IS route for the disappeared IP prefix.
IPQUERY	A clear ip route command was issued on this router.
LSPEXPIRED	Some LSP in the link-state database (LSDB) has expired.
LSPHEADER	ATT/P/OL bits or is-type in an LSP header changed.
NEWADJ	This router has created a new adjacency to another router.
NEWAREA	A new area (via network entity title [NET]) was configured on this router.
NEWLEVEL	A new level (via is-type) was configured on this router.
NEWLSP	A new router or pseudonode appeared in the topology.
NEWMETRIC	A new metric was configured on an interface of this router.
NEWSYSID	A new system ID (via NET) was configured on this router.
PERIODIC	Typically, every 15 minutes a router runs a periodic full SPF calculation.
RTCLEARED	A clear clns route command was issued on this router.
TLVCODE	TLV code mismatch, indicating that different TLVs are included in the newest version of an LSP.
TLVCONTENT	TLV contents changed. This normally indicates that an adjacency somewhere in the area has come up or gone down. The "First trigger LSP" column indicates where the instability may have occurred.

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.

Command	Description
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.

Command	Description
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.

Command	Description
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis topology

To display a list of all connected routers in all areas, use the **show isis topology** command in privileged EXEC mode.

show isis [***| ip** [**unicast**] | **ipv6** [**unicast**]] **topology** [**level-1 | level-2**]

Syntax Description

*****	(Optional) Shows all IS-IS address families.
ip	(Optional) Shows the IPv4 address family.
ipv6	(Optional) Shows the IPv6 address family.
level-1	(Optional) Shows paths to all level-1 routers in the area.
level-2	(Optional) Shows paths to all level-2 routers in the domain.
unicast	(Optional) Shows the unicast address family.

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
9.6(1)	We introduced this command.

Usage Guidelines

Use the **show isis topology** command to verify the presence and connectivity between all routers in all areas.

Examples

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

```
ciscoasa# show isis topology

IS-IS TID 0 paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                  --
routerA                 10           routerA                 subint       0025.8407.f2b0
c3                          10
c2                          10            c2                          subint
c08c.60e6.986f
```

```
IS-IS TID 0 paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                  --
routerA               10           routerA                subint       0025.8407.f2b0
c3                        10
c2                      10           c2                       subint       c08c.60e6.986f
```

Table 8: show isis topology Fields

Field	Description
System Id	Six-byte value that identifies a system in an area.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system [ES], or a CLNS prefix).
Next-Hop	The address of the next hop router.
Interface	Interface from which the system was learned.
SNPA	Subnetwork point of attachment. This is the data-link address.

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.

Command	Description
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.

Command	Description
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show kernel

To display information that the Linux brctl utility provides that you can use for debugging, use the **show kernel** command in privileged EXEC mode.

show kernel [**process | bridge | cgroup-controller | ifconfig | module**]

Syntax Description

bridge	Displays tap bridges.
cgroup-controller	Displays the cgroup-controller statistics.
ifconfig	Displays the tap and bridge interface statistics.
module	Displays the modules that are installed and running.
process	Displays the current status of the active kernel processes running on the ASA.

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
8.0(2)	This command was added.
8.4(1)	The **cgroup-controller** keyword was added.
8.6(1)	The **ifconfig**, **module**, and **bridge** keywords were added.

Usage Guidelines

This command displays statistics for the various processes running on the kernel.

Examples

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

```
ciscoasa# show kernel process
PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
  5    1  20 -5          0        0 3725736671    S        0 kthread
```

```
  7     5  10 -5           0         0 3725736671    S         0 kblockd/0
  8     5  20 -5           0         0 3726794334    S         0 kseriod
 66     5  20  0           0         0 3725811768    S         0 pdflush
 67     5  15  0           0         0 3725811768    S         0 pdflush
 68     1  15  0           0         0 3725824451    S         2 kswapd0
 69     5  20 -5           0         0 3725736671    S         0 aio/0
171     1  16  0      991232        80 3725684979    S         0 init
172   171  19  0      983040       268 3725684979    S         0 rcS
201   172  21  0     1351680       344 3725712932    S         0 lina_monitor
202   201  16  0 1017602048    899932 3725716348    S       212 lina
203   202  16  0 1017602048    899932          0    S         0 lina
204   203  15  0 1017602048    899932          0    S         0 lina
205   203  15  0 1017602048    899932 3725712932    S         6 lina
206   203  25  0 1017602048    899932          0    R 13069390 lina
ciscoasa#
```

Table 9-9 shows each field description.

Table 9: show kernel process Fields

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

Examples

The following example displays output from the **show kernel module** command:

```
ciscoasa# show kernel module
Module                  Size  Used by    Tainted: P
cpp_base              861808  2
kvm_intel              44104  8
kvm                   174304  1 kvm_intel
msrif                   4180  0
tscsync                 3852  0
```

The following example displays output for the **show kernel ifconfig** commands:

ciscoasa# **show kernel ifconfig**

```
br0       Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1708 (1.6 KiB)  TX bytes:0 (0.0 B)
br1       Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
tap0      Link encap:Ethernet  HWaddr 6A:0C:48:32:FE:F4
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:13 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:10320 (10.0 KiB)  TX bytes:12452 (12.1 KiB)
tap1      Link encap:Ethernet  HWaddr 8E:E7:61:CF:E9:BD
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:19368 (18.9 KiB)  TX bytes:14638 (14.2 KiB)
tap2      Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
tap3      Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:187 errors:0 dropped:0 overruns:0 frame:0
          TX packets:256 errors:0 dropped:3 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:14638 (14.2 KiB)  TX bytes:19202 (18.7 KiB)
tap4      Link encap:Ethernet  HWaddr 6A:5C:60:BC:9C:ED
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Related Commands

Command	Description
show module	Shows information about the installed modules in the ASA.

show kernel bridge

To display the Linux bridges, their member ports, and MAC addresses that have been learned at each port that you can use for debugging, use the **show kernel bridge** command in privileged EXEC mode.

show kernel bridge [**mac-address** *bridge name*]

Syntax Description

bridge name	Displays the bridge name.
mac-address	Displays the MAC address associated with each port.

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
8.6(1)	This command was added.

Usage Guidelines

This command shows the Linux bridges, their member ports, and the MAC addresses that have been learned at each port (including remote MAC addresses) that you can use for debugging.

Examples

The following example displays output from the **show kernel bridge** command:

```
ciscoasa# show kernel bridge
bridge name    bridge id        STP enabled interfaces
br0         8000.0e3cd8a8909f    no         tap1
                                tap3
br1        8000.26d29f51a490     no         tap2
                                tap4
                                tap5hostname#
```

The following example displays output from the **show kernel bridge mac-address** command:

```
ciscoasa# show kernel bridge mac-address br1
port no    mac addr       is local?   ageing timer
 1    00:21:d8:cb:dc:f7    no          12.93
 3    00:22:bd:d8:7d:da    no          12.93
 2    26:d2:9f:51:a4:90    yes          0.00
 1    4e:a4:e0:73:1f:ab    yes          0.00
 3    52:04:38:3d:79:c0    yes          0.00
```

Related Commands

Command	Description
show kernel	Shows information about the installed modules in the ASA.

show lacp

To display EtherChannel LACP information such as traffic statistics, system identifier, and neighbor details, enter this command in privileged EXEC mode.

show lacp { [*channel_group_number*] { **counters | internal | neighbor** } **sys-id** }

Syntax Description

channel_group_number	(Optional) Specifies the EtherChannel channel group number, between 1 and 48, and only shows information about this channel group.
counters	Shows counters for the number of LACPDUs and markers sent and received.
internal	Shows internal information.
neighbor	Shows neighbor information.
sys-id	Shows the LACP system ID.

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.

Examples

The following is sample output from the **show lacp sys-id** command:

```
ciscoasa# show lacp sys-id
32768,001c.c4e5.cfee
```

The following is sample output from the **show lacp counters** command:

```
ciscoasa# show lacp counters
            LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv    Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 1
Gi3/1      736    728      0      0        0      0         0
```

```
Gi3/2      739    730      0      0        0      0         0
Gi3/3      739    732      0      0        0      0         0
```

The following is sample output from the **show lacp internal** command:

```
ciscoasa# show lacp internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
Channel group 1
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d
Gi3/2     SA      bndl       32768         0x1       0x1     0x303       0x3d
Gi3/3     SA      bndl       32768         0x1       0x1     0x304       0x3d
```

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

```
ciscoasa# show lacp neighbor
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
Channel group 1 neighbors
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
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

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 lacp cluster

To show the cLACP system MAC and ID, use the **show lacp cluster** command in privileged EXEC mode.

show lacp cluster { **system-mac** | **system-id** }

Syntax Description

system-mac	Shows the system ID and whether it was auto-generated or entered manually.
system-id	Shows the system ID and priority.

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
9.0(1)	This command was added.

Usage Guidelines

Set the cLACP system ID and priority using the **clacp system-mac** command.

Examples

The following is sample output from the **show lacp cluster system-mac** command:

```
ciscoasa(cfg-cluster)# show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

The following is sample output from the **show lacp cluster system-id** command:

```
ciscoasa(cfg-cluster)# show lacp cluster system-id
5    ,a300.010a.010a
```

Related Commands

Command	Description
clacp system-mac	Sets the cLACP system ID and priority.

show license

To show smart licensing status, use the **show license** command in privileged EXEC mode.

Note This feature is supported on the ASA virtual only.

show license [**all | entitlement | cert | pool | registration | features**]

Syntax Description

all	Displays the state of Smart Licensing, Smart Agent version, UDI information, Smart Agent state, global compliance status, the entitlements status, licensing certificate information and schedule Smart Agent tasks.
entitlement	Displays detailed information about each entitlement in use, its handle (i.e. integer id), its count, tag, enforcement mode (e.g. in compliance, out of compliance, etc.), version and time at which the entitlement was requested.
cert	Displays the ID certificate content, date issued, and the date it expires.
pool	Displays the entitlement pool to which this device is assigned.
registration	Displays the current Smart License registration status.
features	Displays the current license.

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
9.3(2)	This command was added.

Usage Guidelines

The **show activation-key** command provides the same output as the show license features command.

Examples

The following example shows an ASA virtual with only a base license (no current license entitlement):

```
Serial Number:  9AAHGX8514R
ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured
Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

show lisp eid

To view the ASA EID table, use the **show lisp eid** command in privileged EXEC mode.

show lisp eid [**site-id** *id*]

Syntax Description

site-id *id*	View only EIDs for a particular site.

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
9.5(2)	This command was added.

Usage Guidelines

The ASA maintains an EID table that correlates the EID and the site ID. View the table with the **show lisp eid** command.

About LISP Inspection for Cluster Flow Mobility

The ASA inspects LISP traffic for location changes and then uses this information for seamless clustering operation. With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

Cluster flow mobility includes several inter-related configurations:

1. (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster. See the **policy-map type inspect lisp**, **allowed-eid,** and **validate-key** commands.
2. LISP traffic inspection—The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. See the **inspect lisp** command.

3. Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers. See the **cluster flow-mobility lisp** command.
4. Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner. See the **site-id** command.
5. Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications. See the **flow-mobility lisp** command.

Examples

The following is sample output from the **show lisp eid** command:

```
ciscoasa# show lisp eid
LISP EID       Site ID
10.44.33.105        2
10.44.33.201        2
192.168.11.1        4
192.168.11.2        4
```

Related Commands

Command	Description
allowed-eids	Limits inspected EIDs based on IP address.
clear cluster info flow-mobility counters	Clears the flow mobility counters.
clear lisp eid	Removes EIDs from the ASA EID table.
cluster flow-mobility lisp	Enables flow mobility for the service policy.
flow-mobility lisp	Enables flow mobility for the cluster.
inspect lisp	Inspects LISP traffic.
policy-map type inspect lisp	Customizes the LISP inspection.
site-id	Sets the site ID for a cluster chassis.
show asp table classify domain inspect-lisp	Shows the ASP table for LISP inspection.
show cluster info flow-mobility counters	Shows flow mobility counters.
show conn	Shows traffic subject to LISP flow-mobility.
show lisp eid	Shows the ASA EID table.
show service-policy	Shows the service policy.
validate-key	Enters the pre-shared key to validate LISP messages.

show local-host

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

show local-host [*hostname* | *ip_address*] [**detail**] [**brief**] [**all**] [**connection** { **sctp | tcp | udp | embryonic** } *start* [*-end*]] [**zone** [*zone_name*]]

Syntax Description

all	(Deprecated) Includes local hosts connecting to the ASA and from the ASA.
brief	(Optional) Displays brief information on local hosts.
connection { **sctp** | **tcp** | **udp** | **embryonic** } *start* [*-end*]	(Deprecated) Applies filters based on the number and type of connections: embryonic, TCP, UDP, or SCTP. The *start* number indicates the minimum number of connections of that type. Include an - *end* number to specify a range, such as 10-100. These filters can be used individually or jointly.
detail	(Optional) Displays the detailed network states of local host information, including more information about active xlates and network connections.
hostname | *ip_address*	(Optional) Specifies the local host name or IPv4/IPv6 address.
zone [*zone_name*]	(Optional) Specifies local hosts per zone.

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)	For models with host limits, this command now shows which interface is considered to be the outside interface.
7.2(4)	Two new options, **connection** and **brief** , were added to the show local-host command so that the output is filtered by the number of connections for the inside hosts.
9.1(2)	The Smart Call Home information sent to Cisco for telemetry-based alerts from the **show local-host** command has been changed to the **show local-host | include interface** command. This provides interface address information.

Release	Modification
9.3(2)	The **zone** keyword was added.
9.5(2)	The display was modified to indicate backup port blocks with an asterisk (*).
9.5(2)	SCTP connections were added to the output. The **connection sctp** keyword was added.
9.14(1)	The connection filter keywords embryonic, TCP, UDP, or SCTP, were deprecated.
9.16(1)	Multicast data connection entries were added to the output.

Usage Guidelines

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

For systems running 9.16 and later, consider using the **show conn address** command instead of this one.

This command lets you show the translation and connection slots for the local hosts. Translation information includes any PAT port blocks allocated to the host.

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

Deprecated Options

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

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

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

Examples

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

```
ciscoasa# show local-host
Interface mgmt: 2 active, 2 maximum active
local host: <10.24.250.191>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
local host: <10.44.64.65>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 1
    TCP intercept watermark = unlimited
    UDP flow count/limit = 5/unlimited
```

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

The following is sample output from the **show local-host** command on an ASA with host limits:

```
ciscoasa# show local-host
Detected interface 'outside' as the Internet interface. Host limit applies to all other
interfaces.
Current host count: 3, towards licensed host limit of: 50
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
```

The following is sample output from the **show local-host** command on an ASA with host limits. But without a default route, the host limits apply to all interfaces. The default route interface might not be detected if the default route or the interface that the route uses is down.

```
ciscoasa# show local-host
Unable to determine Internet interface from default route. Host limit applied to all
interfaces.
Current host count: 3, towards licensed host limit of: 50
Interface c1in: 1 active, 1 maximum active
Interface c1out: 0 active, 0 maximum active
```

The following is sample output from the **show local-host** command on an ASA with unlimited hosts:

```
ciscoasa# show local-host
Licensed host limit: Unlimited
Interface c1in: 1 active, 1 maximum active
Interface c1out: 0 active, 0 maximum active
```

The following example shows information about a specific host, followed by detailed information for that host.

```
ciscoasa# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active
Interface inside: 1 active, 1 maximum active
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)
Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active
ciscoasa# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active
Interface inside: 1 active, 1 maximum active
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri
Conn:
```

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

Related Commands

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

show logging

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

show logging [**message** [*syslog_id* | **all**] | **asdm | queue | setting | flow-export-syslogs**]
message

Syntax Description

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

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)	Indicates whether a syslog server is configured to use an SSL/TLS connection.
8.1(1)	The **flow-export-syslogs** keyword was added.
8.4(1)	For the **show logging** command, the output includes an entry for the current state of the audit block.
9.7(1)	The output from this command includes syslog servers configured with IPv6 addresses.

Usage Guidelines

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

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

- Number of messages that are in the queue
- Highest number of messages recorded that are in the queue
- Number of messages that are discarded because block memory was not available to process them
- Separate queues for traps and other syslog messages

Note The `UDP Tx` in the output displays the number of syslog messages sent from the data engine.

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

Examples

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

```
Timestamp logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 279951603 messages logged
    Trap logging: level debugging, facility 20, 1288748922 messages logged
        Logging to MGMT x.x.x.x errors: 2  dropped: 32
        Logging to MGMT x.x.x.x
        Logging to MGMT x.x.x.x
        Logging to MGMT x.x.x.x errors: 1  dropped: 2
    Permit-hostdown logging: state

    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

Note Valid values of *state* are enabled, disabled, disabled-blocking, and disabled-not blocking.

ASA stores maximum amount of logs per type per minute and drops the rest. You can use the following command to know the configured limit:

```
show running-config all logging | in rate-limit
```

You can modify the limit using `logging rate-limit`.

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

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

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

```
ciscoasa(config)# show logging
            queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

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

```
ciscoasa(config)# show logging message all
syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

The following example shows the messages that are sent to Netflow, and whether they are enabled or disabled.

```
ciscoasa# show logging flow-export-syslogs

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

```
710003          Flow Denied                     Enabled
106100          Flow Created/Denied             Enabled
```

Related Commands

Command	Description
logging asdm	Enables logging to ASDM
logging buffered	Enables logging to the buffer.
logging flow-export-syslogs	Enables or disables syslog messages that are associated with NetFlow data.
logging host	Defines a syslog server.
logging message	Sets the message level or disables messages.
logging queue	Configures the logging queue.

show mac-address-table

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

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

Syntax Description

count	(Optional) Lists the total number of dynamic and static entries.
interface_name	(Optional) Identifies the interface name for which you want to view MAC address table entries.
static	(Optional) Lists only static entries.
vtep-mapping	(Optional) Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.

Command Default

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

Command Modes

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

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.
9.4(1)	The **vtep-mapping** keyword was added.
9.7(1)	Support for routed mode was added.

Examples

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

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

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

```
ciscoasa# show mac-address-table
```

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

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

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

See the following output for the **show mac-address-table vtep-mapping** command:

```
ciscoasa# show mac-address-table vtep-mapping
interface                   mac  address       type     Age(min)   bridge-group    VTEP
-------------------------------------------------------------------------------------------------
vni-outside                00ff.9200.0000      dynamic      5         1        10.9.1.3
vni-inside                 0041.9f00.0000      dynamic      5         1      10.9.1.3
```

Related Commands

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

show mac-learn

To show whether MAC learning is enabled or disabled for each interface, use the **show mac-learn** command in privileged EXEC mode.

show mac-learn

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	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	Support for routed mode was added.

Usage Guidelines

By default, each interface automatically learns the MAC addresses of entering traffic, and the system adds corresponding entries to the MAC address table. You can disable MAC learning per interface.

Examples

The following is sample output from the **show mac-learn** command.

```
ciscoasa# show mac-learn

no mac-learn flood
interface                          mac learn
-----------------------------------------
 outside                             enabled
 inside1_2                           enabled
 inside1_3                           enabled
 inside1_4                           enabled
 inside1_5                           enabled
 inside1_6                           enabled
 inside1_7                           enabled
 inside1_8                           enabled
 diagnostic                          enabled
 inside                              enabled
```

Related Commands

Command	Description
mac-learn	Disables MAC address learning.

show management-access

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

show management-access

Syntax Description

This command has no arguments or keywords.

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

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

Examples

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

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

Related Commands

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

show-map-domain

To show the Mapping Address and Port (MAP) domain, use the **show map-domain** command in privileged EXEC mode.

show map-domain

Command Default

No defaults.

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
9.13(1)	This command was introduced.

Usage Guidelines

The **show map-domain** command displays the MAP configuration (similar to the **show running-config map-domain**), but also indicates whether a domain configuration is valid.

Examples

In the following example, there are two domains, 1 and 2. The output explains that MAP domain 2 is incomplete, and thus it is not active.

```
ciscoasa(config)# show map-domain

MAP Domain 1
  Default Mapping Rule
    IPv6 prefix 2001:db8:cafe:cafe::/64
  Basic Mapping Rule
    IPv6 prefix 2001:cafe:cafe:1::/64
    IPv4 prefix 192.168.3.0 255.255.255.0
    share ratio 16
    start port 1024
    PSID length 4
    PSID offset 6
    Rule EA-bit length 12
MAP Domain 2
  Default Mapping Rule
    IPv6 prefix 2001:db8:1234:1234::/64
Warning: map-domain 2 configuration is incomplete and not in effect.
ciscoasa(config)#
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

show memory

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

show memory [**detail**]

Syntax Description

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

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.
9.2(1)	Virtual machine (VMs) statistics were added to the output to support the ASA virtual.
9.3(2)	The internal memory manager has been replaced by the standard glibc library in the **show memory detail** command.

Usage Guidelines

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

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

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

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

The Free memory is divided into three parts: Heapcache Pool, Global Shared Pool, and System. Heapcache Pool and Global Shared Pool are the amount of free memory available in the glibc heap. System is the available memory that can be allocated from the underlying system. The total amount of Free memory available to the ASA is the sum of Heapcache Pool, Global Shared Pool, and System.

The Used memory is divided into four parts: Heapcache Pool, Global Shared Pool, Reserved, and System Overhead. Heapcache Pool and Global Shared Pool are the amount of Used memory in the glibc heap. Reserved memory (DMA) is the amount of memory reserved for the DMA pools. System overhead is the glibc overhead and process overhead of various running processes.

- Memory is reserved at boot up for DMA and the heapcache.
- Initially, heap memory is allocated from the heapcache, later from the global shared pool once the heapcache is exhausted.
- The global shared pool receives its memory as needed from the system, and returns freed memory back to the system whenever possible.
- The total free heap memory is inclusive of free memory in the system, plus from the heapcache and the global shared pool.

Values displayed in the allocated memory statistics total (bytes) column do not reflect real values (MEMPOOL_GLOBAL_SHARED POOL STATS) in the **show memory detail** command output.

Note Before Version 9.3(2), all system memory (except what goes in DMA pools) appears as part of MEMPOOL_GLOBAL_SHARED. In other words, all allocatable free memory was in MEMPOOL_GLOBAL_SHARED. As of Version 9.3(2), MEMPOOL_GLOBAL_SHARED doesn't take all the system memory during bootup, but asks the underlying operating system for memory whenever required. Similarly, it returns memory to the system when a significant amount of memory is freed. As a result, the size of MEMPOOL_GLOBAL_SHARED appears to grow and shrink according to demand. A minimal amount of free memory remains in MEMPOOL_GLOBAL_SHARED to speed up allocation.

The output shows that the block of size 49,152 was allocated then returned to the free pool, and another block of size 131,072 was allocated. In this case, you would think that free memory decreased by 131,072-49,152=81,920 bytes, but it actually decreased by 100,000 bytes (see the Free memory line).

```
ciscoasa# show memory detail
Free memory heap:                 1193358928 bytes (13%)
Free memory system:               6596267951 bytes (74%)
Used memory:
     Allocated memory in use:      464188448 bytes ( 5%)
     Reserved memory (DMA):        513802240 bytes ( 6%)
     Memory overhead:              202659216 bytes ( 2%)
----------------------------   ------------------
Total memory:                     8970276783 bytes (100%)
Least free memory:       7963442431 bytes (89%)
Most used memory:        1006834352 bytes (11%)
MEMPOOL_HEAPCACHE_0 POOL STATS:
Non-mmapped bytes allocated =   1541406720
Number of free chunks       =          633
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =   1541406720
Keepcost                    =   1190961440
Max contiguous free mem     =   1190961440
Allocated memory in use     =    348047792
Free memory                 =   1193358928
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
```

```
            32           177           5664
            48           204           9792
            64           161          10304
            80             3            240
            96             1             96**
           112             2            224
           160             5            800
           192             1            192
           208             1            208
           224             1            224
           240             1            240
           256            13           4064
           384             2            864
           512             3           1648
          1024             1           1296
         12288             1          13792
         24576             2          57424
         32768             1          43824
         65536             1          65616
        262144             1         322672
       1572864             1        1843712
    1190961440             1     1190961440*
*  - top most releasable chunk.
** - contiguous memory on top of heap.
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
            80          1637         130960
            96         13898        1334208
           112          3422         383264
           128          1910         244480
           144          3677         529488
           160           463          74080
           176           856         150656
           192           357          68544
           208           350          72800
           224           370          82880
           240           337          80880
           256          2293         587008
           384           596         228864
           512           657         336384
           768           504         387072
          1024           449         459776
          1536          1217        1869312
          2048           376         770048
          3072           137         420864
          4096           652        2670592
          6144            73         448512
          8192           212        1736704
         12288           643        7901184
         16384           598        9797632
         24576            31         761856
         32768            77        2523136
         49152            31        1523712
         65536           200       13107200
         98304            30        2949120
        131072            20        2621440
        196608            28        5505024
        262144            14        3670016
        393216            23        9043968
        524288             5        2621440
        786432             9        7077888
       1048576            11       11534336
```

```
      1572864            10       15728640
      2097152             5       10485760
      3145728             3        9437184
      4194304             3       12582912
      6291456             1        6291456
      8388608             1        8388608
     12582912             7       88080384
MEMPOOL_DMA POOL STATS:
Non-mmapped bytes allocated =    513802240
Number of free chunks       =          153
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    513802240
Keepcost                    =    190724944
Max contiguous free mem     =    190724944
Allocated memory in use     =    322994736
Free memory                 =    190807504
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           48            30           1440
           96             1             96**
          112            28           3136
          160             1            160
          208             1            208
          224             1            224
          240             2            480
          256             1            288
          384            19           9104
          512            65          40656
          768             1            800
         1024             2           2608
    190724944             1      190724944*
*  - top most releasable chunk.
** - contiguous memory on top of heap.
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
          160             1            160
          240            92          22080
          256             2            512
          512             2           1024
         1024           163         166912
         2048             5          10240
         8192             1           8192
        12288            18         221184
        16384             1          16384
        32768            38        1245184
        49152             1          49152
        65536             1          65536
       131072             4         524288
       196608             3         589824
       262144             8        2097152
       393216             6        2359296
       524288             2        1048576
       786432             1         786432
      1048576            11       11534336
      1572864             7       11010048
      3145728             8       25165824
      6291456             5       31457280
      8388608             1        8388608
     12582912             7       88080384
```

```
MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated =       135168
Number of free chunks       =            4
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =            0
Keepcost                    =        51616
Max contiguous free mem     =        51616
Allocated memory in use     =         4064
Free memory                 =       131104
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
          432             1             432
        40960             1           50848
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           96             1              96
          112             1             112
          160             1             160
          208             3             624
Summary for all pools:
Non-mmapped bytes allocated =   2055344128
Number of free chunks       =          790
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =   2055208960
Keepcost                    =   1381738000
Allocated memory in use     =    671046592
Free memory                 =   1384297536
```

The following output confirms that a block of size 149,0327 was allocated, instead of 131,072:

```
ciscoasa# show memory binsize 131072
MEMPOOL_HEAPCACHE_0 pool bin stats:
pc = 0x7f739a97db9f, size = 1490327  , count = 9
pc = 0x7f7399be30a0, size = 309008   , count = 2
pc = 0x7f7399be31f4, size = 1255704  , count = 9
MEMPOOL_DMA pool bin stats:
pc = 0x7f73984ba38d, size = 323486   , count = 2
pc = 0x7f73984b8e55, size = 320286   , count = 2
MEMPOOL_GLOBAL_SHARED pool bin stats:
```

The approximate number of total bytes shown in the **show memory detail** command output is by design. There are two reasons for this:

- For each fragment size, if you had to get the sum of all fragments, a performance impact would occur because there can be very large number of allocations for a single fragment size and to get the accurate value, you need to walk over thousands of chunks.
- For each binsize, you need to walk through the doubly linked list of allocations and there could be many allocations. In this case, you cannot hog the CPU for an extended period and would need to suspend allocations periodically. After you resume allocations, other processes may have allocated or deallocated memory and memory states may have changed. As a result, the total bytes column gives an approximate value instead of the real value.

Examples

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

```
ciscoasa# show memory
Free memory:        3208100250 bytes (72%)
Used memory:        1247711232 bytes (28%)
-------------     ------------------
Total memory:       4455811482 bytes (100%)
```

Note: Free memory is the free system memory. Additional memory maybe available from memory pools internal to the ASA process. Use show memory detail command to view this information, but use it carefully since it may cause CPU hogs and packet loss under load.

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

```
ciscoasa# show memory detail
Heap Memory:
   Free Memory:
      Heapcache Pool:                     447109376 bytes ( 10% )
      Global Shared Pool:                    131152 bytes (  0% )
      System:                           3208100250 bytes ( 72% )
   Used Memory:
      Heapcache Pool:                     257533696 bytes (  6% )
      Global Shared Pool:                      4016 bytes (  0% )
      Reserved (Size of DMA Pool):        234881024 bytes (  5% )
      System Overhead:                    308051968 bytes (  7% )
-----------------------------------     ----------------
   Total Memory:                        4455811482 bytes ( 100% )
Warning:  The information reported here is computationally expensive to
          determine, and may result in CPU hogs and performance impact.
-------------------------------------------------------------------------------
MEMPOOL_HEAPCACHE_0 POOL STATS:
Non-mmapped bytes allocated =    704643072
Number of free chunks       =          309
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    704643072
Keepcost                    =    446723584
Max contiguous free mem     =    446723584
Allocated memory in use     =    257533696
Free memory                 =    447109376
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           32            91           2912
           48           116           5568
           64            83           5312
           96             1             96**
           96             3            288
          112             1            112
          160             2            320
          224             2            448
          240             1            240
          256             2            544
          384             1            384
          512             2           1392
          768             2           1904
        32768             1          44704
    446723584             1      446723584*
*  - top most releasable chunk.
** - contiguous memory on top of heap.
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
```

```
----------------  ----------  --------------
            80          937           74960
            96        10758         1032768
           112         2051          229712
           128          898          114944
           144         2887          415728
           160          290           46400
           176          300           52800
           192          164           31488
           208          246           51168
           224          183           40992
           240          208           49920
           256         1396          357376
           384          474          182016
           512          305          156160
           768          322          247296
          1024          240          245760
          1536          321          493056
          2048          171          350208
          3072           45          138240
          4096          259         1060864
          6144           47          288768
          8192          174         1425408
         12288           94         1155072
         16384          571         9355264
         24576           17          417792
         32768           51         1671168
         49152           16          786432
         65536          121         7929856
         98304           14         1376256
        131072            9         1179648
        196608           19         3735552
        262144           12         3145728
        393216           15         5898240
        524288            2         1048576
        786432            9         7077888
       1048576           12        12582912
       1572864            5         7864320
       2097152            3         6291456
       3145728            2         6291456
       4194304            4        16777216
       6291456            3        18874368
       8388608            1         8388608
      12582912            3        37748736
MEMPOOL_DMA POOL STATS:
Non-mmapped bytes allocated =    234881024
Number of free chunks       =          162
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    234881024
Keepcost                    =     90103152
Max contiguous free mem     =     90103152
Allocated memory in use     =    144701888
Free memory                 =     90179136
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
            96             1             96**
           112             1            112
           256            64          20480
           384            32          15360
           512            64          39936
      90103152             1       90103152*
```

```
*  - top most releasable chunk.
** - contiguous memory on top of heap.
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
          160             2             320
          256             2             512
          512             1             512
         1024           160          163840
         2048             5           10240
         8192             1            8192
        12288            18          221184
        16384             1           16384
        32768            37         1212416
        49152             2           98304
        65536             1           65536
       131072             4          524288
       196608             2          393216
       262144             4         1048576
       393216             2          786432
       524288             2         1048576
       786432             1          786432
      1048576             3         3145728
      1572864             2         3145728
      3145728             3         9437184
      6291456             2        12582912
     12582912             3        37748736
MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated =       135168
Number of free chunks       =            4
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =            0
Keepcost                    =        96368
Max contiguous free mem     =        96368
Allocated memory in use     =         4016
Free memory                 =       131152
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
          448             1            448
        20480             1          23296
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           96             1             96
          112             1            112
          160             1            160
          192             3            576
Summary for all pools:
Non-mmapped bytes allocated =    939659264
Number of free chunks       =          475
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    939524096
Keepcost                    =    536923104
Allocated memory in use     =    402239600
Free memory                 =    537419664
On 5585:
========
ciscoasa# show memory
```

```
Free memory:        4544618496 bytes (73%)
Used memory:        1714343936 bytes (27%)
-------------     ------------------
Total memory:       6258962432 bytes (100%)
Note: Free memory is the free system memory. Additional memory may
      be available from memory pools internal to the ASA process.
      Use 'show memory detail' to see this information, but use it
      with care since it may cause CPU hogs and packet loss under load.
ciscoasa# show memory detail
Heap Memory:
   Free Memory:
      Global Shared Pool:                  283589104 bytes (  5% )
      System:                             4544618496 bytes ( 73% )
   Used Memory:
      Global Shared Pool:                   41813520 bytes (  1% )
      Reserved (Size of DMA Pool):         445095936 bytes (  7% )
      System Overhead:                     943845376 bytes ( 15% )
-----------------------------------     ----------------
   Total Memory:                       6258962432 bytes ( 100% )
Warning:  The information reported here is computationally expensive to
          determine, and may result in CPU hogs and performance impact.
------------------------------------------------------------------------
MEMPOOL_DMA POOL STATS:
Non-mmapped bytes allocated =    445095936
Number of free chunks       =          161
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    445095936
Keepcost                    =    250149264
Max contiguous free mem     =    250149264
Allocated memory in use     =    194871536
Free memory                 =    250224400
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           64             1             64
           96             1             96**
          112             1            112
          256            63          20192
          384            32          15360
          512            63          39312
    250149264             1      250149264*
*  - top most releasable chunk.
** - contiguous memory on top of heap.
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           80             1             80
          144             1            144
          160             2            320
          256             2            512
          512             1            512
         1024           160         163840
         2048             5          10240
         8192             5          40960
        12288            27         331776
        16384             1          16384
        32768            39        1277952
        49152             1          49152
        65536             1          65536
        98304             4         393216
       131072             4         524288
```

```
       196608             1         196608
       262144             3         786432
       393216             2         786432
       524288             2        1048576
       786432             5        3932160
      1048576             3        3145728
      1572864             2        3145728
      3145728             4       12582912
     12582912             4       50331648
MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated =     43286528
Number of free chunks       =          474
Number of mmapped regions   =          156
Mmapped bytes allocated     =    282116096
Max memory footprint        =            0
Keepcost                    =        11200
Max contiguous free mem     =       132816
Allocated memory in use     =     41813520
Free memory                 =      1473008
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           32          135           4320
           48          203           9744
           64           38           2432
           80            2            160
           80           20           1600
           96            3            288
           96            3            288
          112           90          10080
          112           10           1120
          128           20           2560
          144            1            144
          240            1            240
          384            1            384
          400            1            400
          448            1            448
          480            1            480
          544            1            544
          560            6           3360
          656            1            656
          816            1            816
          832            1            832
          880            1            880
         1088            3           3360
         1664            1           1680
         3136            1           3280
         3584            1           3776
         8704            1           8704
        24576            1          25728
        40960            1          50064

----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           64          354          22656
           80         1234          98720
           96        12337        1184352
          112         1202         134624
          128          970         124160
          144         2777         399888
          160          435          69600
```

```
          176           155          27280
          192           323          62016
          208           250          52000
          224            86          19264
          240           388          93120
          256          1478         378368
          384           304         116736
          512           304         155648
          768           314         241152
         1024           410         419840
         1536          1188        1824768
         2048           136         278528
         3072            42         129024
         4096           814        3334144
         6144            56         344064
         8192           174        1425408
        12288           123        1511424
        16384           584        9568256
        24576            30         737280
        32768            60        1966080
        49152            30        1474560
        65536           139        9109504
        98304            25        2457600
       131072            19        2490368
       196608            32        6291456
       262144            18        4718592
       393216            29       11403264
       524288             7        3670016
       786432             8        6291456
      1048576            13       13631488
      1572864            11       17301504
      2097152             6       12582912
      3145728             2        6291456
      4194304             4       16777216
      8388608             1        8388608
     12582912             6       75497472
Summary for all pools:
Non-mmapped bytes allocated =    488382464
Number of free chunks       =          635
Number of mmapped regions   =            0
Mmapped bytes allocated     =    282116096
Max memory footprint        =    445095936
Keepcost                    =    250160464
Allocated memory in use     =    236685056
Free memory                 =    251697408
```

The following is sample output from the **show memory** command on the ASA 5525 after enabling the **jumbo-frame reservation** command and issuing the **write memory** command and the **reload** command:

```
ciscoasa# show memory
Free memory:        3208100250 bytes (72%)
Used memory:        1247711232 bytes (28%)
-------------     ------------------
Total memory:       4455811482 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5525 without enabling the **jumbo-frame reservation** command:

```
ciscoasa# show memory
Free memory:        3208100250 bytes (72%)
Used memory:        1247711232 bytes (28%)
```

```
-------------     ------------------
Total memory:       4455811482 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5515 after enabling the **jumbo-frame reservation** command:

```
ciscoasa# show memory
Free memory:        3276619472 bytes (76%)
Used memory:        1018347824 bytes (24%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5515 without enabling the **jumbo-frame reservation** command:

```
ciscoasa# show memory
Free memory:        3481145472 bytes (81%)
Used memory:         813821824 bytes (19%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5585 after enabling the **jumbo-frame reservation** command:

```
ciscoasa# show memory
Free memory:        8883297824 bytes (69%)
Used memory:        4001604064 bytes (31%)
-------------       ------------------
Total memory:      12884901888 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5585 without enabling the **jumbo-frame reservation** command:

```
ciscoasa# show memory
Free memory:        9872205104 bytes (77%)
Used memory:        3012696784 bytes (23%)
-------------       ------------------
Total memory:      12884901888 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5520, which does not support the **jumbo-frame** command:

```
ciscoasa# show memory
ree memory:         206128232 bytes (38%)
Used memory:         330742680 bytes (62%)
-------------       -----------------
Total memory:        536870912 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5505, which does not support the **jumbo-frame** command:

```
ciscoasa# show memory
Free memory:          48457848 bytes (18%)
Used memory:         219977608 bytes (82%)
-------------        -----------------
Total memory:        268435456 bytes (100%
```

The following is sample output from the **show memory** command on the ASA virtual:

```
Free memory:        2694133440 bytes (63%)
Used memory:        1600833856 bytes (37%)
-------------      ------------------
Total memory:       4294967296 bytes (100%)
Virtual platform memory
-----------------------
Provisioned       4096 MB
Allowed           4096 MB
Status            Compliant
```

Related Commands

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

show memory all

To display a summary of the maximum physical memory and current free memory available to the operating system, use the **show memory all** command in privileged EXEC mode. This value includes lina and snort memory usage.

show memory all

Command History

Release	Modification
9.16(1)	This command was introduced.

Usage Guidelines

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

```
ciscoasa#show memory all
Data Path:
Free memory:        3161408675 bytes (72%)
Used memory:        1203826208 bytes (28%)
-------------     ------------------
Total memory:       4365234883 bytes (100%)
Inspection Engine:
Free memory:                  0 bytes ( 0%)
Used memory:                  0 bytes ( 0%)
-------------     ------------------
Total memory:                 0 bytes (100%)
System:
Free memory:                  0 bytes ( 0%)
Used memory:                  0 bytes ( 0%)
-------------     ------------------
Total memory:                 0 bytes (100%)
ciscoasa#
```

show memory api

To display the malloc stack APIs that are registered in the system, use the **show memory api** command in privileged EXEC mode.

show memory api

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command displays the malloc stack APIs that are registered in the system.

If any of the memory debugging features are turned on (that is, delay-free-poisoner, memory tracker, or memory profiler), their APIs appear in the **show memory api** command output.

Examples

This following is sample output from the **show memory api** command:

```
ciscoasa# show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

Related Commands

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

show memory app-cache

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

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

Syntax Description

access-list	(Optional) Shows the application level memory cache for access lists.
detail	(Optional) Shows a detailed view of free and allocated system memory.
flow	(Optional) Shows the application level memory cache for flows.
host	(Optional) Shows application level memory cache for hosts.
http	(Optional) Shows application level memory cache for HTTP.
tcb	(Optional) Shows application level memory cache for TCB.
tcb-ips	(Optional) Shows application level memory cache for TCB-IPS.
threat-detection	(Optional) Shows application level memory cache for threat detection.

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
8.0(1)	This command was added.
8.1(1)	The **access-list** and **http** options were added.
9.10(1)	The tcb-ips option was added.

Usage Guidelines

This command enables you to observe memory usage by application.

Examples

The following is sample output from the **show memory app-cache threat-detection** command:

```
ciscoasa(config)# show memory app-cache threat-detection
```

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

The following is sample output from the **show memory app-cache threat-detection detail** command:

```
ciscoasa(config)# show memory app-cache threat-detection detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
TD ACE stats 50 0 2 0 1936
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host stats 50 50 16120 0 116515360
TD Subnet stats 50 2 113 0 207016
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

The following is sample output from the **show memory app-cache host detail** command:

```
ciscoasa(config)# show memory app-cache host detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Host Core 0 1000 1000 5116 0 961808
SNP Host Core 1 1000 1000 4968 0 933984
SNP Host Core 2 1000 1000 5413 0 1017644
SNP Host Core 3 1000 1000 4573 0 859724
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 20070 0 3773160
```

The following is sample output from the **show memory app-cache flow detail** command:

```
ciscoasa(config)# show memory app-cache flow detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn Core 0 1000 1000 893 0 639388
SNP Conn Core 1 1000 948 980 0 701680
SNP Conn Core 2 1000 1000 1175 0 841300
SNP Conn Core 3 1000 1000 901 0 645116
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 3948 3949 0 2827484
```

The following is sample output from the **show memory app-cache access-list detail** command:

```
ciscoasa(config)# show memory app-cache access-list detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
NP ACL log c Core 0 1000 0 1 0 68
NP ACL log c Core 1 1000 0 6 0 408
NP ACL log c Core 2 1000 0 19 0 1292
NP ACL log c Core 3 1000 0 0 0 0
NP ACL log f Core 0 1000 0 0 0 0
NP ACL log f Core 1 1000 0 0 0 0
NP ACL log f Core 2 1000 0 0 0 0
NP ACL log f Core 3 1000 0 0 0 0
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 26 0 1768
```

The following is sample output from the **show memory app-cache http detail** command:

```
ciscoasa(config)# show memory app-cache http detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
Inspect HTTP Core 0 1000 0 0 0 0
Inspect HTTP Core 1 1000 0 0 0 0
Inspect HTTP Core 2 1000 0 0 0 0
Inspect HTTP Core 3 1000 0 0 0 0
HTTP Result Core 0 1000 0 0 0 0
HTTP Result Core 1 1000 0 0 0 0
HTTP Result Core 2 1000 0 0 0 0
HTTP Result Core 3 1000 0 0 0 0
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 0 0 0
```

The following is sample output from the **show memory app-cache tcb detail** command:

```
ciscoasa(config)# show memory app-cache tcb detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB Core 0 1000 1000 968 0 197472
SNP TCB Core 1 1000 1000 694 0 141576
SNP TCB Core 2 1000 1000 1304 0 266016
SNP TCB Core 3 1000 1000 1034 0 210936
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 4000 0 816000
```

The following is sample output from the **show memory app-cache tcb-ips detail** command:

```
ha-asa5512a(config)# show memory app-cache tcb-ips detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB IPS Core 00     625 0 0 0 0
LIMIT      COUNT      ALLOC     FAILED   BYTES USED
TOTAL         625          0 0 0            0
ha-asa5512a(config)# show memory app-cache
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
[...]
SNP TCB IPS Core 00 625 0 0 0 0
SNP TCB IPS Total 625 0 0 0 0
[...]
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 61972 149 188 0        50212
```

Related Commands

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

show memory appcache-threshold

To display the status and hit count of memory appcache-threshold, use the show memory appcache-threshold command in the privileged EXEC mode.

show memory appcache-threshold

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

Command History

Release	Modification
9.10(1)	This command was introduced.

Usage Guidelines

Use **show memory appcache-threshold** command to display the hit count and status of memory allocation threshold for a managed application.

Examples

The following example displays the memory appcache threshold status for a managed application:

```
ciscoasa# show memory appcache-threshold
          CACHE NAME   STATUS      THRESHOLD     HIT COUNT
    SNP Conn Core 00   ENABLED            85             5

ciscoasa# show memory appcache-threshold
          CACHE NAME   STATUS      THRESHOLD     HIT COUNT
    SNP Conn Core 00   DISABLED           85             5
```

Table 10: show memory appcache-threshold Fields

Field	Description
Cache Name	The name of the managed application cache. For ASA 9.10.1 release, only the SNP Conn Core 00 application cache type is managed.
Status	Whether the appcache-threshold feature on this application cache type is enabled or disabled.
Threshold	The threshold of this application cache type. For example, 85 means 85% of the system memory used.

Field	Description
Hit Count	The number of times this threshold being hit since the counter was cleared last time.

Related Commands

Command	Description
memory appcache-threshold enable	Enable memory appcache-threshold to restrict application cache allocations after reaching certain memory threshold
clear memory appcache-threshold	Clear the hit count of memory appcache-threshold

show memory binsize

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

show memory binsize *size*

Syntax Description

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

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
7.2(1)	This command was added.

Usage Guidelines

This command has no usage guidelines.

Examples

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

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

Related Commands

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

show memory caller-address

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

show memory caller-address

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

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

Examples

The following examples show how to configure the address ranges with the **memory caller-address** command, and the resulting output of the **show memory-caller address** command:

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

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

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

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

Related Commands

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

show memory delayed-free-poisoner

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

show memory delayed-free-poisoner

Syntax Description

This command has no arguments or keywords.

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
7.0(1)	This command was added.

Usage Guidelines

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

Examples

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

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

Table 9-11 describes the significant fields in the **show memory delayed-free-poisoner** command output.

Table 11: show memory delayed-free-poisoner Command Output Descriptions

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

Related Commands

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

show memory logging

To display the memory usage for logging, use the **show memory logging** command in privileged EXEC mode.

show memory logging [**brief | wrap | include** [**address**] [**caller**] [**operator**] [**size**] [**process**] [**time**] [**context**]]

Syntax Description

address	(Optional) Displays address information.
brief	(Optional) Displays abbreviated memory usage logging.
caller	(Optional) Displays caller information.
context	(Optional) Displays virtual context information.
include	Includes only the specified fields in the output. You can specify the fields in any order, but they always appear in the following order: **1.** Process **2.** Time **3.** Context (unless in single mode) **4.** Operation (free/malloc/etc.) **5.** Address **6.** Size **7.** Callers The output format is: process=[XXX] time=[XXX] context=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX Up to four caller addresses appear. The types of operations are listed in the output (Number of...) shown in the example.
operator	(Optional) Displays operator information.
process	(Optional) Displays process information.
size	(Optional) Displays size information.
time	(Optional) Displays time information.
wrap	(Optional) Displays memory usage logging wrapped data, which is purged after you enter this command so that duplicate data does not appear and is not saved.

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
9.4(1)	This command was introduced.

Usage Guidelines

The show memory logging command shows log memory allocations and memory usage, and lets you respond to memory logging wrap events.

Examples

```
The following is sample output from the show memory logging
command on the ASA:
ciscoasa# show memory logging
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] time=[13:26:33.407] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542 0x000000000131911a

0x0000000000442bfd process=[ci/console] time=[13:26:33.407] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542 0x000000000182774d

0x000000000182cc8a process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542 0x0000000000bfef9a

0x0000000000bff606 process=[CMGR Server Process] time=[13:26:35.964] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000021246ef 0x0000000001827098 0x000000000182c08d

0x000000000182c262 process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff224b9460 size=40 @ 0x00000000021246ef 0x000000000182711b 0x000000000182c08d
```

```
0x000000000182c262 process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542 0x000000000182774d

0x000000000182cc8a process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542 0x0000000000bfef9a

0x0000000000bff606 process=[CMGR Server Process] time=[13:26:38.464] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[ci/console] time=[13:26:38.557] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542 0x000000000131911a

0x0000000000442bfd process=[ci/console] time=[13:26:38.557] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b
The following is sample output from the show memory logging include process operation size

command on the ASA:
ciscoasa# show memory logging include process operation size
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free] size=72 process=
[CMGR Server Process] oper=[malloc] size=16 process=[CMGR Server Process] oper=[malloc]
size=512 process=[CMGR Server Process] oper=[free] size=512 process=[CMGR Server Process]
oper=[malloc] size=40 process=[CMGR Server Process] oper=[free] size=16 process=[CMGR Server

Process] oper=[free] size=40 process=[CMGR Server Process] oper=[malloc] size=16 process=[CMGR

Server Process] oper=[malloc] size=512 process=[CMGR Server Process] oper=[free] size=512
process=[CMGR Server Process] oper=[malloc] size=40 process=[ci/console] oper=[malloc]
size=72
process=[ci/console] oper=[free] size=72
The following is sample output from the show memory logging brief
command on the ASA:
ciscoasa# show memory logging brief
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
```

Related Commands

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

show memory profile

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

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

Syntax Description

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

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
7.0(1)	This command was added.

Usage Guidelines

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

Note The ASA might experience a temporary reduction in performance when memory profiling is enabled.

Examples

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

```
ciscoasa# show memory profile

Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

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

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

```
ciscoasa# show memory profile detail

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

The following is sample output from the **show memory profile collated** command:

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

The following is sample output from the **show memory profile peak** command, which shows the peak capture buffer:

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

The following is sample output from the **show memory profile peak detail** command, which shows the peak capture buffer and the number of bytes that is held by the text/code that falls in the corresponding bucket address:

```
ciscoasa# show memory profile peak detail

Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

The following is sample output from the **show memory profile status** command, which shows the current state of memory profiling and the peak capture buffer:

```
ciscoasa# show memory profile status

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

Related Commands

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

show memory region

To show the processes maps, use the **show memory region** command in privileged EXEC mode.

show memory region

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

Use the **show memory region** command shows the processes memory map.

Examples

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

```
ciscoasa# show memory region
ASLR enabled, text region 7f7397701000-7f739bc186c4
Address Perm Offset Dev Inode Pathname
7f7391a06000-7f7391d09000 rw-p 00000000 00:00 0 [stack:2161]
7f7391d2a000-7f739212e000 rw-p 00000000 00:00 0 [stack:2157]
7f7392530000-7f7392631000 rw-p 00000000 00:00 0 [stack:2156]
7f7392647000-7f7392849000 rw-p 00000000 00:00 0 [stack:2154]
7f7392895000-7f7392897000 r-xp 00000000 00:01 989 /lib64/libutil-2.18.so
7f7392897000-7f7392a96000 ---p 00002000 00:01 989 /lib64/libutil-2.18.so
7f7392a96000-7f7392a97000 r--p 00001000 00:01 989 /lib64/libutil-2.18.so
7f7392a97000-7f7392a98000 rw-p 00002000 00:01 989 /lib64/libutil-2.18.so
7f7392a98000-7f7392c9a000 r-xp 00000000 00:01 2923 /usr/lib64/libcrypto.so.1.0.0
7f7392c9a000-7f7392e99000 ---p 00202000 00:01 2923 /usr/lib64/libcrypto.so.1.0.0
```

7f7392e99000-7f7392ec3000 rw-p 00201000 00:01 2923 /usr/lib64/libcrypto.so.1.0.0
7f7392ec7000-7f7392f28000 r-xp 00000000 00:01 3114 /usr/lib64/libssl.so.1.0.0
7f7392f28000-7f7393127000 ---p 00061000 00:01 3114 /usr/lib64/libssl.so.1.0.0
7f7393127000-7f7393132000 rw-p 00060000 00:01 3114 /usr/lib64/libssl.so.1.0.0
7f7393132000-7f739316a000 r-xp 00000000 00:01 3202 /usr/lib64/libxslt.so.1.1.28
7f739316a000-7f739336a000 ---p 00038000 00:01 3202 /usr/lib64/libxslt.so.1.1.28
7f739336a000-7f739336c000 rw-p 00038000 00:01 3202 /usr/lib64/libxslt.so.1.1.28
7f739336c000-7f73933ca000 r-xp 00000000 00:01 3439 /usr/lib64/libxmlsec1.so.1.2.20
7f73933ca000-7f73935ca000 ---p 0005e000 00:01 3439 /usr/lib64/libxmlsec1.so.1.2.20
7f73935ca000-7f73935ce000 rw-p 0005e000 00:01 3439 /usr/lib64/libxmlsec1.so.1.2.20
7f73935ce000-7f7393606000 r-xp 00000000 00:01 2950 /usr/lib64/libxmlsec1-openssl.so.1.2.20
7f7393606000-7f7393805000 ---p 00038000 00:01 2950 /usr/lib64/libxmlsec1-openssl.so.1.2.20
7f7393805000-7f7393809000 rw-p 00037000 00:01 2950 /usr/lib64/libxmlsec1-openssl.so.1.2.20
7f739380a000-7f7393811000 r-xp 00000000 00:01 2976 /usr/lib64/libffi.so.6.0.1
7f7393811000-7f7393a11000 ---p 00007000 00:01 2976 /usr/lib64/libffi.so.6.0.1
7f7393a11000-7f7393a12000 rw-p 00007000 00:01 2976 /usr/lib64/libffi.so.6.0.1
7f7393a12000-7f7393b94000 r-xp 00000000 00:01 2929 /usr/lib64/libpython2.7.so.1.0
7f7393b94000-7f7393d94000 ---p 00182000 00:01 2929 /usr/lib64/libpython2.7.so.1.0
7f7393d94000-7f7393dd3000 rw-p 00182000 00:01 2929 /usr/lib64/libpython2.7.so.1.0
7f7393de1000-7f7393df6000 r-xp 00000000 00:01 948 /lib64/libz.so.1.2.8
7f7393df6000-7f7393ff5000 ---p 00015000 00:01 948 /lib64/libz.so.1.2.8
7f7393ff5000-7f7393ff6000 rw-p 00014000 00:01 948 /lib64/libz.so.1.2.8
7f7393ff6000-7f739419a000 r-xp 00000000 00:01 961 /lib64/libc-2.18.so
7f739419a000-7f7394399000 ---p 001a4000 00:01 961 /lib64/libc-2.18.so
7f7394399000-7f739439d000 r--p 001a3000 00:01 961 /lib64/libc-2.18.so
7f739439d000-7f739439f000 rw-p 001a7000 00:01 961 /lib64/libc-2.18.so
7f73943a3000-7f73943b8000 r-xp 00000000 00:01 949 /lib64/libgcc_s.so.1
7f73943b8000-7f73945b8000 ---p 00015000 00:01 949 /lib64/libgcc_s.so.1
7f73945b8000-7f73945b9000 rw-p 00015000 00:01 949 /lib64/libgcc_s.so.1
7f73945b9000-7f73946bb000 r-xp 00000000 00:01 999 /lib64/libm-2.18.so
7f73946bb000-7f73948ba000 ---p 00102000 00:01 999 /lib64/libm-2.18.so
7f73948ba000-7f73948bb000 r--p 00101000 00:01 999 /lib64/libm-2.18.so
7f73948bb000-7f73948bc000 rw-p 00102000 00:01 999 /lib64/libm-2.18.so
7f73948bc000-7f73948be000 r-xp 00000000 00:01 3641 /asa/lib/libplatcap.so

7f73948be000-7f7394abd000 ---p 00002000 00:01 3641 /asa/lib/libplatcap.so
7f7394abd000-7f7394ac5000 rw-p 00001000 00:01 3641 /asa/lib/libplatcap.so
7f7394ac5000-7f7394b12000 r-xp 00000000 00:01 3213 /usr/lib64/libgobject-2.0.so.0.3600.4
7f7394b12000-7f7394d12000 ---p 0004d000 00:01 3213 /usr/lib64/libgobject-2.0.so.0.3600.4
7f7394d12000-7f7394d14000 rw-p 0004d000 00:01 3213 /usr/lib64/libgobject-2.0.so.0.3600.4
7f7394d14000-7f7394e3d000 r-xp 00000000 00:01 3120 /usr/lib64/libglib-2.0.so.0.3600.4
7f7394e3d000-7f739503d000 ---p 00129000 00:01 3120 /usr/lib64/libglib-2.0.so.0.3600.4
7f739503d000-7f739503f000 rw-p 00129000 00:01 3120 /usr/lib64/libglib-2.0.so.0.3600.4
7f739503f000-7f73950ce000 r-xp 00000000 00:01 3143 /usr/lib64/liblasso.so.3.11.1
7f73950ce000-7f73952ce000 ---p 0008f000 00:01 3143 /usr/lib64/liblasso.so.3.11.1
7f73952ce000-7f73952d9000 rw-p 0008f000 00:01 3143 /usr/lib64/liblasso.so.3.11.1
7f73952d9000-7f73952e9000 r-xp 00000000 00:01 3175 /usr/lib64/libprotobuf-c.so.0.0.0
7f73952e9000-7f73954e8000 ---p 00010000 00:01 3175 /usr/lib64/libprotobuf-c.so.0.0.0
7f73954e8000-7f73954e9000 rw-p 0000f000 00:01 3175 /usr/lib64/libprotobuf-c.so.0.0.0
7f73954e9000-7f739551b000 r-xp 00000000 00:01 3629 /asa/lib/libmsglyr.so
7f739551b000-7f739571b000 ---p 00032000 00:01 3629 /asa/lib/libmsglyr.so
7f739571b000-7f7395720000 rw-p 00032000 00:01 3629 /asa/lib/libmsglyr.so
7f7395720000-7f739576c000 r-xp 00000000 00:01 3146 /usr/lib64/libzmq.so.3.1.0
7f739576c000-7f739596c000 ---p 0004c000 00:01 3146 /usr/lib64/libzmq.so.3.1.0
7f739596c000-7f7395970000 rw-p 0004c000 00:01 3146 /usr/lib64/libzmq.so.3.1.0
7f7395970000-7f7395ac0000 r-xp 00000000 00:01 2952 /usr/lib64/libxml2.so.2.9.1
7f7395ac0000-7f7395cc0000 ---p 00150000 00:01 2952 /usr/lib64/libxml2.so.2.9.1
7f7395cc0000-7f7395cca000 rw-p 00150000 00:01 2952 /usr/lib64/libxml2.so.2.9.1
7f7395ccb000-7f7395ceb000 r-xp 00000000 00:01 3628 /asa/lib/libpdts.so
7f7395ceb000-7f7395eea000 ---p 00020000 00:01 3628 /asa/lib/libpdts.so
7f7395eea000-7f7395eec000 rw-p 0001f000 00:01 3628 /asa/lib/libpdts.so
7f7395eec000-7f7395eff000 r-xp 00000000 00:01 2057 /lib64/libresolv-2.18.so
7f7395eff000-7f73960ff000 ---p 00013000 00:01 2057 /lib64/libresolv-2.18.so
7f73960ff000-7f7396100000 r--p 00013000 00:01 2057 /lib64/libresolv-2.18.so
7f7396100000-7f7396101000 rw-p 00014000 00:01 2057 /lib64/libresolv-2.18.so
7f7396103000-7f7396110000 r-xp 00000000 00:01 955 /lib64/libudev.so.0.13.1
7f7396110000-7f739630f000 ---p 0000d000 00:01 955 /lib64/libudev.so.0.13.1
7f739630f000-7f7396310000 rw-p 0000c000 00:01 955 /lib64/libudev.so.0.13.1
7f7396310000-7f7396322000 r-xp 00000000 00:01 964 /lib64/libcgroup.so.1.0.38

7f7396322000-7f7396521000 ---p 00012000 00:01 964 /lib64/libcgroup.so.1.0.38
7f7396521000-7f7396523000 rw-p 00011000 00:01 964 /lib64/libcgroup.so.1.0.38
7f739677d000-7f7396784000 r-xp 00000000 00:01 2067 /lib64/librt-2.18.so
7f7396784000-7f7396983000 ---p 00007000 00:01 2067 /lib64/librt-2.18.so
7f7396983000-7f7396984000 r--p 00006000 00:01 2067 /lib64/librt-2.18.so
7f7396984000-7f7396985000 rw-p 00007000 00:01 2067 /lib64/librt-2.18.so
7f7396985000-7f7396988000 r-xp 00000000 00:01 2060 /lib64/libdl-2.18.so
7f7396988000-7f7396b87000 ---p 00003000 00:01 2060 /lib64/libdl-2.18.so
7f7396b87000-7f7396b88000 r--p 00002000 00:01 2060 /lib64/libdl-2.18.so
7f7396b88000-7f7396b89000 rw-p 00003000 00:01 2060 /lib64/libdl-2.18.so
7f7396b89000-7f7396ba2000 r-xp 00000000 00:01 1001 /lib64/libpthread-2.18.so
7f7396ba2000-7f7396da1000 ---p 00019000 00:01 1001 /lib64/libpthread-2.18.so
7f7396da1000-7f7396da2000 r--p 00018000 00:01 1001 /lib64/libpthread-2.18.so
7f7396da2000-7f7396da3000 rw-p 00019000 00:01 1001 /lib64/libpthread-2.18.so
7f7396da7000-7f7396dce000 r-xp 00000000 00:01 3434 /usr/lib64/libexpat.so.1.6.0
7f7396dce000-7f7396fcd000 ---p 00027000 00:01 3434 /usr/lib64/libexpat.so.1.6.0
7f7396fcd000-7f7396fd0000 rw-p 00026000 00:01 3434 /usr/lib64/libexpat.so.1.6.0
7f7396fd0000-7f73970b6000 r-xp 00000000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73970b6000-7f73972b5000 ---p 000e6000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73972b5000-7f73972bd000 r--p 000e5000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73972bd000-7f73972bf000 rw-p 000ed000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73972d4000-7f73972de000 r-xp 00000000 00:01 3174 /usr/lib64/libnuma.so.1
7f73972de000-7f73974dd000 ---p 0000a000 00:01 3174 /usr/lib64/libnuma.so.1
7f73974dd000-7f73974de000 rw-p 00009000 00:01 3174 /usr/lib64/libnuma.so.1
7f73974de000-7f73974fe000 r-xp 00000000 00:01 950 /lib64/ld-2.18.so
7f73976fe000-7f73976ff000 r--p 00020000 00:01 950 /lib64/ld-2.18.so
7f73976ff000-7f7397700000 rw-p 00021000 00:01 950 /lib64/ld-2.18.so
7f7397701000-7f739bc19000 r-xp 00000000 00:01 3650 /asa/bin/lina
7f739be18000-7f739cc16000 rw-p 04517000 00:01 3650 /asa/bin/lina
7ffffe1fc000-7ffffe21d000 rw-p 00000000 00:00 0 [stack]
7ffffe2f1000-7ffffe2f3000 r-xp 00000000 00:00 0 [vdso]

Related Commands

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

show memory top-usage

To display the top number of allocated fragment sizes from the **show memory detail** command, use the **show memory top-usage** command in privileged EXEC mode.

show memory top-usage [*num*]

Syntax Description

num	(Optional) Shows the number of bin sizes to list. Valid values are from 1-64.

Command Default

The default for *num* is 10.

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(6)	This command was added.

Usage Guidelines

Use the **show memory top-usage** command to display the top number of allocated fragment sizes from the **show memory detail** command.

This command does not use clustering and does not need to be disabled when clustering is enabled.

Examples

The following is sample output from the show memory top-usage command:

```
ciscoasa# show memory top-usage 3
MEMPOOL_DMA pool binsize allocated byte totals:
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
      1572864             9       14155776
     12582912             1       12582912
      6291456             1        6291456
----- Binsize PC top usage -----
Binsize: 1572864                total (bytes): 14155776
pc = 0x805a870, size = 16422399 , count = 9
Binsize: 12582912               total (bytes): 12582912
pc = 0x805a870, size = 12960071 , count = 1
Binsize: 6291456                total (bytes): 6291456
pc = 0x9828a6c, size = 7962695  , count = 1
MEMPOOL_GLOBAL_SHARED pool binsize allocated byte totals:
----- allocated memory statistics -----
```

```
 fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
     12582912             1       12582912
      2097152             6       12582912
        65536           181       11862016
----- Binsize PC top usage -----
Binsize: 12582912               total (bytes): 12582912
pc = 0x8249763, size = 37748736 , count = 1
Binsize: 2097152                total (bytes): 12582912
pc = 0x8a7ebfb, size = 2560064  , count = 1
pc = 0x8aa4413, size = 2240064  , count = 1
pc = 0x8a9bb13, size = 2240064  , count = 1
pc = 0x8a80542, size = 2097152  , count = 1
pc = 0x97e7172, size = 2097287  , count = 1
pc = 0x8996463, size = 2272832  , count = 1
Binsize: 65536                  total (bytes): 11862016
pc = 0x913db2b, size = 11635232 , count = 161
pc = 0x91421eb, size = 138688   , count = 2
pc = 0x97e7172, size = 339740   , count = 4
pc = 0x97e7433, size = 197229   , count = 3
pc = 0x82c3412, size = 65536    , count = 1
pc = 0x8190e09, size = 155648   , count = 2
pc = 0x8190af6, size = 77824    , count = 1
pc = 0x93016a1, size = 65536    , count = 1
pc = 0x89f1a40, size = 65536    , count = 1
pc = 0x9131140, size = 163968   , count = 2
pc = 0x8ee56c8, size = 66048    , count = 1
pc = 0x8056a01, size = 66528    , count = 1
pc = 0x80569e5, size = 66528    , count = 1
```

Related Commands

Command	Description
show memory tracking	Shows all currently collected information.

show memory tracking

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

show memory tracking [**address | dump | detail**]

Syntax Description

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

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	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

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

Examples

The following is sample output from the show memory tracking command:

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

The following is sample output from the show memory tracking address command:

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

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

The following is sample output from the show memory tracking dump command:

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

Related Commands

Command	Description
clear memory tracking	Clears all currently collected information.

show memory utilization

Use the show memory utilization command to view the configured reload threshold limit and the crash information on ASA.

show memory-utilization [**reload-threshold**]

Syntax Description

reload-threshold	Displays the configured system memory reload threshold limit, and if crash information is saved before a system reload.

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	• Yes	• Yes	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

Use the **show memory utilization** command to know if a reload threshold is configured. If configured, you can view the threshold limit and whether the optional choice to save crash information before a reload is set.

Examples

The following example displays how to configure memory utilization feature on ASA:

```
ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is not configured.
ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is configured:
Reload at: 93%
Crashinfo Generation: yes
ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is configured:
Reload at: 90%
Crashinfo Generation: no
```

show memory webvpn

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

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

Syntax Description

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

usedobjects	Displays WebVPN memory consumption details for used objects.

Command Default

No default behavior or value.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was added.

Examples

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

```
ciscoasa
#
 show memory webvpn
            allobjects

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

Related Commands

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

show mfib

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

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

Syntax Description

cluster	(Optional) Displays the MFIB epoch number and the current timer value.
group	(Optional) Displays the IP address of the multicast group.
source	(Optional) Displays the IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.
verbose	(Optional) Displays additional information about the entries.

Command Default

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

Command Modes

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

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.
9.0(1)	The **cluster** keyword was added. Applies to the ASA 5580 and 5585-X only.

Examples

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

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

Related Commands

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

show mfib active

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

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

Syntax Description

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

This command has no arguments or keywords.

Command Default

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

Command Modes

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

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

Examples

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

```
ciscoasa# show mfib active
Active IP Multicast Sources - sending >= 4 kbps
Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)
Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)
Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

Related Commands

Command	Description
show mroute active	Displays active multicast streams.

show mfib count

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

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

Syntax Description

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

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 displays packet drop statistics.

Examples

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

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

Related Commands

Command	Description
clear mfib counters	Clears MFIB router packet counters.

Command	Description
show mroute count	Displays multicast route counters.

show mfib interface

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

show mfib interface [*interface*]

Syntax Description

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

Command Default

Information for all MFIB 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.

Examples

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

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

Related Commands

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

show mfib reserved

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

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

Syntax Description

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

Command Default

The default value for *kbps* is 4.

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 MFIB entries in the range 224.0.0.0 through 224.0.0.225.

Examples

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

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

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

Related Commands

Command	Description
show mfib active	Displays active multicast streams.

show mfib status

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

show mfib status

Syntax Description

This command has no arguments or keywords.

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.

Examples

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

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

Related Commands

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

show mfib summary

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

show mfib summary

Syntax Description

This command has no arguments or keywords.

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.

Examples

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

```
ciscoasa# show mfib summary
IPv6 MFIB summary:
  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]
  17     total MFIB interfaces
```

Related Commands

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

show mfib verbose

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

show mfib verbose

Syntax Description

This command has no arguments or keywords.

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.

Examples

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

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

Related Commands

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

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

show mgcp

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

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

Syntax Description

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

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
7.0(1)	This command was added.

Usage Guidelines

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

Examples

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

```
ciscoasa# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
ciscoasa#
ciscoasa# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
Gateway IP | host-pc-2
Transaction ID  2052
Endpoint name | aaln/1
Call ID | 9876543210abcdef
Connection ID |
Media IP | 192.168.5.7
Media port | 6058
```

```
ciscoasa#
ciscoasa# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
ciscoasa#
ciscoasa# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
Gateway IP | host-pc-2
Call ID | 9876543210abcdef
Connection ID | 6789af54c9
Endpoint name | aaln/1
Media lcl port  6166
Media rmt IP | 192.168.5.7
Media rmt port  6058
ciscoasa#
```

Related Commands

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

show mmp

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

show mmp [*address*]

Syntax Description

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

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
8.0(4)	This command was added.

Examples

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

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

Related Commands

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

show mode

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

show mode

Syntax Description

This command has no arguments or keywords.

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.

Examples

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

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

The mode can be multiple or single.

Related Commands

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

show module

To show information about a module installed on the ASA, use the **show module** command in user EXEC mode.

show module [*id* | **all**] [**details | recover | log** [**console**]]

Syntax Description

all	(Default) Shows information for all modules.
console	(Optional) Shows console log information for the module.
details	(Optional) Shows additional information, including remote management configuration for modules.
id	Specifies the module ID. For a hardware module, specify the slot number, which can be **0** (for the ASA) or **1** (for an installed module). For a software module, specify one of the following names: • **sfr** —ASA FirePOWER module. • **ips** —IPS module • **cxsc** —ASA CX module
log	(Optional) Shows log information for the module.
recover	(Optional) Shows the settings for the **hw-module** or **sw-module module recover** command.

Command Default

By default, information for all modules 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	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was modified to include more detail in the output.
8.2(1)	Information about the SSC is included in the output.
8.2(5)	Information about support for the ASA 5585-X and for the IPS SSP on the ASA 5585-X was added.
8.4(4.1)	Support for the ASA CX module was added.

Release	Modification
8.6(1)	For the ASA 5512-X through ASA 5555-X the **log** and **console** keywords were added; the **ips** device ID was added.
9.1(1)	Support for the ASA CX software module was added by adding the **cxsc** module ID.
9.2(1)	Support for the ASA FirePOWER module, including the **sfr** keyword was added.

Usage Guidelines

This command shows information about the modules installed in the ASA. The ASA itself also appears as a module in the display (in slot 0).

Examples

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

```
ciscoasa# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0
Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c30d to 000b.fcf8.c311  1.0          1.0(10)0     7.1(0)5
  1 000b.fcf8.012c to 000b.fcf8.012c  1.0          1.0(10)0     CSC SSM 5.0 (Build#1187)
Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
  1 CSC SSM scan services are not
  1 CSC SSM                        5.0 (Build#1187)
Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

The following table describes each field listed in the output.

Table 12: show module Output Fields

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

Field	Description
Sw Version	The software version.
SSM Application Name	The name of the application running on the SSM.
SSM Application Version	The version of the application running on the SSM.
Status	For the device in module 0, the status is Up Sys. The status of the SSM in module 1 can be any of the following: • Initializing—The SSM is being detected and the control communication is being initialized by the device. • Up—The SSM has completed initialization by the device. • Unresponsive—The device encountered an error while communicating with this SSM. • Reloading—The SSM is reloading. • Shutting Down—The SSM is shutting down. • Down—The SSM is shut down. • Recover—The SSM is attempting to download a recovery image. • No Image Present—The IPS software has not been installed.
Data Plane Status	The current state of the data plane.
Compatibility	The compatibility of the SSM relative to the rest of the device.
Slot	The physical slot number (used only in dual SSP mode).

The output of the **show module details** command varies according to which module is installed. For example, output for the CSC SSM includes fields about components of the CSC SSM software.

The following is generic sample output from the **show module 1 details** command:

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

The following table describes the additional fields in the output.

Table 13: show module details Additional Output Fields

Field	Description
DC address (not shown)	(ASA FirePOWER only). The address of the management center that manages the module.
Mgmt IP addr	Shows the IP address for the module's management interface.
Mgmt Network Mask (not shown)	Shows the subnet mask for the management address.
Mgmt Gateway (not shown)	The gateway for the management address.
Mgmt web ports	Shows the ports configured for the module's management interface.
Mgmt TLS enabled	Shows whether transport layer security is enabled (true or false) for connections to the management interface of the module.

For models that allow you to configure software modules, the **show module** command lists all possible modules. Status information indicates whether one of them is installed.

```
ciscoasa# show module

Mod  Card Type                                    Model              Serial No.
---- -------------------------------------------- ------------------ -----------
   0 ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt     ASA5555            FCH1714J6HP
 ips Unknown                                      N/A                FCH1714J6HP
cxsc Unknown                                      N/A                FCH1714J6HP
 sfr FirePOWER Services Software Module           ASA5555            FCH1714J6HP
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 bc16.6520.1dcd to bc16.6520.1dd6  1.0          2.1(9)8      100.8(66)11
 ips bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A
cxsc bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A
 sfr bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A          5.3.1-100
Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
 ips Unknown                        No Image Present Not Applicable
cxsc Unknown                        No Image Present Not Applicable
 sfr ASA FirePOWER                  Up               5.3.1-100
Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
 ips Unresponsive       Not Applicable
cxsc Unresponsive       Not Applicable
 sfr Up                 Up
Mod  License Name   License Status  Time Remaining
---- -------------- --------------- ---------------
 ips IPS Module     Enabled         172 days
```

The following is sample output from the **show module 1 recover** command:

```
ciscoasa# show module 1 recover
Module 1 recover parameters. . .
```

```
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

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

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

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

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

The following is sample output from the **show module all** command when a CXSC SSP is installed in an ASA 5585-X:

```
ciscoasa# show module all
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------  ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi  ASA5585-SSP-10     JAF1504CBRM
  1 ASA 5585-X CXSC Security Services Processor-1 ASA5585-SSP-IPS10  JAF1510BLSE
Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 5475.d05b.1d54 to 5475.d05b.1d5f  1.0          2.0(7)0      100.7(14)13
  1 5475.d05b.248c to 5475.d05b.2497  1.0          0.0(0)0      1.0
Mod SSM Application Name           Status           SSM Application Version
```

```
--- ------------------------------ ---------------- --------------------------
  1 CXSC Security Module             Up               1.0
Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

The following is sample output from the **show module 1 details** command when a CXSC SSP is installed in an ASA 5585-X:

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA5585-S10C10-K8
Hardware version:   1.0
Serial Number:      123456789
Firmware version:   1.0(9)0
Software version:   CXSC Security Module Version 1.0
App. name:          CXSC Security Module
App. version:       Version 1.0
Data plane Status:  Up
Status:             Up
HTTP Service:       Up
Activated:          Yes
Mgmt IP addr:       100.0.1.4
Mgmt web port:      8443
```

Related Commands

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

show monitor-interface

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

show monitor-interface

Syntax Description

This command has no arguments or keywords.

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.
8.2(2)	IPv6 addresses were added to the output.

Usage Guidelines

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

Monitored failover interfaces can have the following status:

- Unknown—Initial status. This status can also mean the status cannot be determined.
- Normal—The interface is receiving traffic.
- Normal (Waiting)—The interface is up but has not yet received a hello packet from the corresponding interface on the peer unit. Verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
- Testing—Hello messages are not heard on the interface for five poll times.
- Link Down—The interface or VLAN is administratively down.
- No Link—The physical link for the interface is down.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

Examples

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

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

Related Commands

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

show mrib client

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

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

Syntax Description

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

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

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

Examples

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

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

```
include All
igmp:77964 (connection id 1)
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

Related Commands

Command	Description
show mrib route	Displays MRIB table entries.

show mrib route

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

show mmp [[*source* |*] [*group* [/ *prefix-length*]]]

Syntax Description

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

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

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

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

Examples

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

```
ciscoasa# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
```

```
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS
(*,224.0.0.0/24) Flags: D
(*,224.0.1.39) Flags: S
(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI
(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A
(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

Related Commands

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

show mroute

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

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

Syntax Description

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

Command Default

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

Command Modes

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

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.

Usage Guidelines

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

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

Examples

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

```
ciscoasa(config)# show mroute
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State
(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never
(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

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

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

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

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

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

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

Related Commands

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