show diameter peer through show object-group

show device-sensor cache

To display device sensor cache entries, use the **show device-sensor cache** command in privileged EXEC mode.

show device-sensor cache {**mac** *mac-address* | **all**}

Syntax Description

mac *mac-address*	Specifies the MAC address of the device for which the sensor cache entries are to be displayed.
all	Displays sensor cache entries for all devices.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)SE1	This command was introduced.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.

Usage Guidelines

Use the **show device-sensor cache** command to display a list of Type-Length-Value (TLV) fields or options received from a particular device or from all devices.

Examples

The following is sample output from the **show device-sensor cache mac** *mac-address* command:

```
Device# show device-sensor cache mac 0024.14dc.df4d

Device: 0024.14dc.df4d on port GigabitEthernet1/0/24
-----------------------------------------------
Proto   Type:Name                       Len Value
cdp     26:power-available-type          16 00 1A 00 10 00 00 00 01 00 00 00 00 FF FF FF FF
cdp     22:mgmt-address-type             17 00 16 00 11 00 00 00 01 01 01 CC 00 04 09 1B 65
                                            0E
cdp     11:duplex-type                    5 00 0B 00 05 01
cdp      9:vtp-mgmt-domain-type           4 00 09 00 04
cdp      4:capabilities-type              8 00 04 00 08 00 00 00 28
cdp      1:device-name                   14 00 01 00 0E 73 75 70 70 6C 69 63 61 6E 74
lldp     0:end-of-lldpdu                  2 00 00
lldp     8:management-address            14 10 0C 05 01 09 1B 65 0E 03 00 00 00 01 00
lldp     7:system-capabilities            6 0E 04 00 14 00 04
lldp     4:port-description              23 08 15 47 69 67 61 62 69 74 45 74 68 65 72 6E 65
                                            74 31 2F 30 2F 32 34
lldp     5:system-name                   12 0A 0A 73 75 70 70 6C 69 63 61 6E 74
dhcp    82:relay-agent-info              20 52 12 01 06 00 04 00 18 01 18 02 08 00 06 00 24
                                            14 DC DF 80
dhcp    12:host-name                     12 0C 0A 73 75 70 70 6C 69 63 61 6E 74
dhcp    61:client-identifier             32 3D 1E 00 63 69 73 63 6F 2D 30 30 32 34 2E 31 34
                                            64 63 2E 64 66 34 64 2D 47 69 31 2F 30 2F 32 34
```

```
dhcp    57:max-message-size             4 39 02 04 80
```

The following is sample output from the **show device-sensor cache all** command:

```
Device# show device-sensor cache all

Device: 001c.0f74.8480 on port GigabitEthernet2/1
----------------------------------------------
Proto   Type:Name                       Len  Value
dhcp    52:option-overload               3  34 01 03
dhcp    60:class-identifier             11  3C 09 64 6F 63 73 69 73 31 2E 30
dhcp    55:parameter-request-list        8  37 06 01 42 06 03 43 96
dhcp    61:client-identifier            27  3D 19 00 63 69 73 63 6F 2D 30 30 31 63 2E 30 66
                                            37 34 2E 38 34 38 30 2D 56 6C 31
dhcp    57:max-message-size              4  39 02 04 80

Device: 000f.f7a7.234f on port GigabitEthernet2/1
----------------------------------------------
Proto   Type:Name                       Len  Value
cdp     22:mgmt-address-type             8  00 16 00 08 00 00 00 00
cdp     19:cos-type                      5  00 13 00 05 00
cdp     18:trust-type                    5  00 12 00 05 00
cdp     11:duplex-type                   5  00 0B 00 05 01
cdp     10:native-vlan-type              6  00 0A 00 06 00 01
cdp      9:vtp-mgmt-domain-type          9  00 09 00 09 63 69 73 63 6F
```

The following table describes the significant fields shown in the display.

Table 1: show device-sensor global Field Descriptions

Field	Description
Device	MAC address of the device and the interface that it is connected to.
Proto	Protocol from which the endpoint device data is being gleaned.
Type	Type of TLV.
Name	Name of the TLV.
Len	Length of the TLV.
Value	Value of the TLV.

Related Commands

Command	Description
debug device-sensor	Enables debugging for device sensor.
device-sensor accounting	Adds the device sensor protocol data to accounting records and generates additional accounting events when new sensor data is detected.
device-sensor filter-list cdp	Creates a Cisco Discovery Protocol filter containing a list of options that can be included or excluded in the device sensor output.

Command	Description
device-sensor filter-list dhcp	Creates a DHCP filter containing a list of options that can be included or excluded in the device sensor output.
device-sensor filter-list lldp	Creates an LLDP filter containing a list of TLV fields that can be included or excluded in the device sensor output.
show device-sensor cache	Displays device sensor cache entries.

show diameter peer

To display the configuration and status of a specific Diameter peer, or all Diameter peers, use the **show diameter peer** command in privileged EXEC mode.

show diameter peer [*peer-name*]

Syntax Description

peer- name	Displays the configuration and status of the specified Diameter peer. **Note** If no peer name is specified, the command will display information for all configured Diameter peers.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command displays the peer status information, as well as counters, including:

- Total packets sent
- Total responses seen
- Packets with responses
- Packets without responses
- Average response delay (ms)
- Number of Diameter timeouts
- Buffer allocation failures

Examples

The following is a sample output from the **show diameter peer command**:

```
Router#
show diameter peer iwan-view5
Peer information for iwan-view5
------------------------------
Peer name: iwan-view 5
Peer type: Server
Peer transport protocol: TCP
Peer listening port: 3688
Peer security protocol: IPSEC
Peer connection timer value: 30 seconds
```

```
Peer watch dog timer value: 35 seconds
Peer vrf name: default
Peer connection status: UP
```

The fields shown above are self-explanatory.

Related Commands

Command	Description
debug diameter	Displays information about the Diameter protocol.

show dmvpn

To display Dynamic Multipoint VPN (DMVPN)-specific session information, use the **show dmvpn** command in privileged EXEC mode.

show dmvpn [**ipv4** [**vrf** *vrf-name*]| **ipv6** [**vrf** *vrf-name*]] [**debug-condition**| **interface tunnel** *number*| **peer** {**nbma** {*ipv4-address*| *ipv6-address*}| **network** *network-mask*| **tunnel** *ip-address*}| **static**| **detail**]

Syntax Description

ipv4	(Optional) Displays information about IPv4 private networks.
vrf *vrf-name*	(Optional) Displays information based on the specified virtual routing and forwarding (VRF) instance.
ipv6	(Optional) Displays information about IPv6 private networks.
debug-condition	(Optional) Displays DMVPN conditional debugging.
interface	(Optional) Displays DMVPN information based on a specific interface.
tunnel	(Optional) Displays DMVPN information based on the peer Virtual Private Network (VPN) address.
number	(Optional) The tunnel address for a DMVPN peer.
peer	(Optional) Displays information for a specific DMVPN peer.
nbma	Displays DMVPN information based on nonbroadcast multiaccess (NBMA) addresses.
ipv4-address	The DMVPN peer IPv4 address.
ipv6-address	The DMVPN peer IPv6 address.
network *network-mask*	Displays DMVPN information based on a specific destination network and mask address.
static	(Optional) Displays only static DMVPN information.
detail	(Optional) Displays detail DMVPN information for each session, including Next Hop Server (NHS) and NHS status, crypto session information, and socket details.

Command Default Information is displayed for all DMVPN-specific sessions.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	This command was modified. The following were added: **ipv4**, **ipv6**, *ipv6-address*, **network,**and *ipv6-address*.
12.4(22)T	This command was modified. The output of this command was extended to display the NHRP group received from the spoke and the Quality of Service (QoS) policy applied to the spoke tunnel.
15.2(1)T	This command was modified. The*ipv6-address* argument was added.

Usage Guidelines Use this command to obtain DMVPN-specific session information. By default, summary information will be displayed.

When the **detail** keyword is used, command output will include information from the **show crypto session detail** command, including inbound and outbound security parameter indexes (SPIs) and the **show crypto socket** command.

Examples The following example shows sample summary output:

```
Device# show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
! The line below indicates that the sessions are being displayed for Tunnel1.
! Tunnel1 is acting as a spoke and is a peer with three other NBMA peers.
Tunnel1, Type: Spoke, NBMA Peers: 3,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2    192.0.2.21       192.0.2.116   IKE     3w0d D
     1    192.0.2.102      192.0.2.11   NHRP 02:40:51 S
     1    192.0.2.225      192.0.2.10     UP     3w0d S
Tunnel2, Type: Spoke, NBMA Peers: 1,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1      192.0.2.25     192.0.2.171   IKE    never S
```

The table below describes the significant fields shown in the display.

Table 2: show dmvpn Field Descriptions

Field	Description
# Ent	The number of Next Hop Routing Protocol (NHRP) entries in the current session.
Peer NBMA Addr	The remote NBMA address.
Peer Tunnel Add	The remote tunnel endpoint IP address.
State	The state of the DMVPN session. The DMVPN session is either up or down. If the DMVPN state is down, the reason for the down state error is displayed--Internet Key Exchange (IKE), IPsec, or NHRP.
UpDn Tm	Displays how long the session has been in the current state.
Attrib	Displays any associated attributes of the current session. One of the following attributes will be displayed--dynamic (D), static (S), incomplete (I), Network Address Translation (NAT) for the peer address, or NATed, (N), local (L), no socket (X).

The following example shows sample summary output of the **show dmvpn** command with IPv6 information:

```
Device# show dmvpn

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

  Ent  Peer NBMA Addr        Peer Tunnel Add   State   UpDn Tm     Attrb
 ----- ---------------       ---------------   -----    --------  -----
     1 2001:DB8:0:ABCD::1    10.255.255.254    IKE      05:55:30   S

Interface: Tunnel0, IPv6 NHRP Details
Type:Spoke, Total NBMA Peers (v4/v6): 1
    1.Peer NBMA Address: 2001:DB8:0:ABCD::1
        Tunnel IPv6 Address: 2001:DB8:0:FFFF::1
        IPv6 Target Network: 2001:DB8:A:B::1/64
         Ent: 1, Status: IKE, UpDn Time: 05:55:30, Cache Attrib: S
```

In this example output the first line displays only tunnel count and peer NBMA address entries irrespective of the IPv6 address length. Other entries are displayed in the immediate next line. When you use **show dmvpn detail** command and in case if there are two tunnel entries with same NBMA address in the command output, tunnel count “0” in the second entry is not displayed and the extra line is removed between the entries in the output.

The following example shows output of the **show dmvpn** command with the **detail** keyword:

```
Device# show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
```

```
        # Ent --> Number of NHRP entries with same NBMA peer
-------------- Interface Tunnel1 info: --------------
Intf. is up, Line Protocol is up, Addr. is 192.0.2.5
   Source addr: 192.0.2.229, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "gre_prof",
Tunnel VRF "" ip vrf forwarding ""
NHRP Details: NHS: 192.0.2.10 RE 192.0.2.11  E
Type: Spoke, NBMA Peers: 4
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    2        192.0.2.21      192.0.2.116    UP 00:14:59 D      192.0.2.118/24
                                            UP 00:14:59 D      192.0.2.116/32
  IKE SA: local 192.0.2.229/500 remote 192.0.2.21/500 Active
          Capabilities:(none) connid:1031 lifetime:23:45:00
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.21
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 1 drop 0 life (KB/Sec) 4494994/2700
        Outbound: #pkts enc'ed 1 drop 0 life (KB/Sec) 4494994/2700
   Outbound SPI : 0xD1EA3C9B, transform : esp-3des esp-sha-hmac
    Socket State: Open
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1     192.0.2.229       192.0.2.5    UP 00:15:00 DLX        192.0.2.5/32
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1     192.0.2.102      192.0.2.11 NHRP 02:55:47  S         192.0.2.11/32
  IKE SA: local 192.0.2.229/4500 remote 192.0.2.102/4500 Active
          Capabilities:N connid:1028 lifetime:11:45:37
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.102
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 199056 drop 393401 life (KB/Sec) 4560270/1524
        Outbound: #pkts enc'ed 416631 drop 10531 life (KB/Sec) 4560322/1524
   Outbound SPI : 0x9451AF5C, transform : esp-3des esp-sha-hmac
    Socket State: Open
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1     192.0.2.225      192.0.2.10    UP     3w0d S         192.0.2.10/32
  IKE SA: local 192.0.2.229/500 remote 192.0.2.225/500 Active
          Capabilities:(none) connid:1030 lifetime:03:46:44
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.225
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 430261 drop 0 life (KB/Sec) 4415197/3466
        Outbound: #pkts enc'ed 406232 drop 4 life (KB/Sec) 4415197/3466
   Outbound SPI : 0xAF3E15F2, transform : esp-3des esp-sha-hmac
    Socket State: Open
 -------------- Interface Tunnel2 info: --------------
Intf. is up, Line Protocol is up, Addr. is 192.0.2.172
   Source addr: 192.0.2.20, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "gre_prof",
Tunnel VRF "" ip vrf forwarding ""
NHRP Details: NHS:         192.0.2.171  E
Type: Spoke, NBMA Peers: 1
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      192.0.2.25     192.0.2.171  IKE     never S        192.0.2.171/32
  IKE SA: local 192.0.2.20/500 remote 192.0.2.25/500 Inactive
          Capabilities:(none) connid:0 lifetime:0
  IKE SA: local 192.0.2.20/500 remote 192.0.2.25/500 Inactive
          Capabilities:(none) connid:0 lifetime:0
  Crypto Session Status: DOWN-NEGOTIATING
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.20 host 192.0.2.25
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 436431 life (KB/Sec) 0/0
   Outbound SPI : 0x       0, transform :
    Socket State: Closed
```

```
Pending DMVPN Sessions:
!There are no pending DMVPN sessions.
```

The following example shows output of the **show dmvpn** command with the **detail** keyword. This example displays the NHRP group received from the spoke and the QoS policy applied to the spoke tunnel:

```
Device# show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
 -------------- Interface Tunnel0 info: --------------
Intf. is up, Line Protocol is up, Addr. is 10.0.0.1
   Source addr: 172.17.0.1, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "dmvpn-profile",
Tunnel VRF "", ip vrf forwarding ""
NHRP Details:
Type:Hub, NBMA Peers:2
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      172.17.0.2        10.0.0.2    UP 00:19:57 D           10.0.0.2/32
NHRP group: test-group-0
 Output QoS service-policy applied: queueing
  IKE SA: local 172.17.0.1/500 remote 172.17.0.2/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 172.17.0.2
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.2
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x44E4E634, transform : esp-des esp-sha-hmac
    Socket State: Open
  IKE SA: local 172.17.0.1/500 remote 172.17.0.2/500 Active
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.2
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x44E4E634, transform : esp-des esp-sha-hmac
    Socket State: Open
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      172.17.0.3        10.0.0.3    UP 00:02:21 D           10.0.0.3/32
NHRP group: test-group-0
 Output QoS service-policy applied: queueing
  IKE SA: local 172.17.0.1/500 remote 172.17.0.3/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 172.17.0.3
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.3
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0xBF13C9CC, transform : esp-des esp-sha-hmac
    Socket State: Open
  IKE SA: local 172.17.0.1/500 remote 172.17.0.3/500 Active
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.3
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0xBF13C9CC, transform : esp-des esp-sha-hmac
    Socket State: Open
 -------------- Interface Tunnel1 info: --------------
Intf. is up, Line Protocol is up, Addr. is 11.0.0.1
   Source addr: 172.17.0.1, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "dmvpn-profile",
Tunnel VRF "", ip vrf forwarding ""
NHRP Details:
Type:Hub, NBMA Peers:1
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      172.17.0.2        11.0.0.2    UP 00:20:01 D           11.0.0.2/32
NHRP group: test-group-1
 Output QoS service-policy applied: queueing
Pending DMVPN Sessions:
```

The following example shows DMVPN debug-condition information:

```
Device#  show dmvpn debug-condition

NBMA addresses under debug are:
Interfaces under debug are:
```

```
Tunnel101,
Crypto DMVPN filters:
Interface = Tunnel101
DMVPN Conditional debug context unmatched flag: OFF
```

Related Commands

Command	Description
debug dmvpn	Debugs DMVPN sessions.
show crypto session detail	Displays detailed status information for active crypto sessions.
show crypto socket	Lists crypto sockets.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

show dnsix

To display state information and the current configuration of the DNSIX audit writing module, use the **show dnsix**command in privil eged EXEC mode.

show dnsix

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
Router# show dnsix

Audit Trail Enabled with Source 192.168.2.5
          State: PRIMARY
          Connected to 192.168.2.4
          Primary 192.168.2.4
          Transmit Count 1
          DMDP retries 4
          Authorization Redirection List:
               192.168.2.4
          Record count: 0
          Packet Count: 0
          Redirect Rcv: 0
```

show dot1x

To display details for an identity profile, use the **show dot1x** command in privileged EXEC mode.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **show dot1x** command is supplemented by the **show authentication** command. The **show dot1x** command is reserved for displaying output specific to the use of the 802.1X authentication method. The **show authentication sessions**command has a wider remit of displaying information for all authentication methods and authorization features. See the **show authentication sessions**command for more information.

show dot1x [**all [summary]**| **interface** *interface-name*| **details**| **statistics**]

Syntax Description

all	(Optional) Displays 802.1X status for all interfaces.
summary	(Optional) Displays summary of 802.1X status for all interfaces.
interface *interface-name*	(Optional) Specifies the interface name and number.
details	(Optional) Displays the interface configuration as well as the authenticator instances on the interface.
statistics	(Optional) Displays 802.1X statistics for all the interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(11)AX	This command was introduced.
12.1(14)EA1	The **all** keyword was added.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)SED	The output display was expanded to include auth-fail-vlan information in the authorization state machine state and port status fields.
12.2(25)SEE	The **details** and **statistics** keywords were added.

Release	Modification
12.3(11)T	The PAE, HeldPeriod, StartPeriod, and MaxStart fields were added to the **show dot1x** command output.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear in the output.

Note In some IOS versions, the **show dot1x** command may not display the AUTHORIZED or UNAUTHORIZED value in the Port Status command output field if authentication methods other than the 802.1X authentication method are used. If the Port Status field does not contain a value, then use the **show authentication sessions** command to display the Authz Success or Authz Failed port status authentication value.

Examples

The following is sample output from the **show dot1x** command using both the **interface** and **details** keywords. The clients are successfully authenticated in this example.

```
Router# show dot1x interface ethernet1/0 details
Dot1x Info for Ethernet1/0
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 1
TxPeriod                  = 30
Dot1x Authenticator Client List
-------------------------------
Supplicant                = aabb.cc00.c901
Session ID                = 0A3462800000000000009F8
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
```

The following is sample output from the **show dot1x** command using both the **interface** and **details** keywords. The clients are unsuccessful at authenticating in this example.

```
Router# show dot1x interface ethernet1/0 details
Dot1x Info for Ethernet1/0
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 1
```

```
TxPeriod                  = 30
Dot1x Authenticator Client List Empty
```

The table below describes the significant fields shown in the displays.

Table 3: show dot1x Field Descriptions

Field	Description
PAE	Port Access Entity. Defines the role of an interface (as a supplicant, as an authenticator, or as an authenticator and supplicant).
PortControl	Port control value. • AUTO--The authentication status of the client PC is being determined by the authentication process. • Force-authorize--All the client PCs on the interface are being authorized. • Force-unauthorized--All the client PCs on the interface are being unauthorized.
ControlDirection	Indicates whether control for an IEEE 802.1X controlled port is applied to both directions (ingress and egress), or inbound direction only (ingress). See 'dot1x control-direction', or effective from Cisco IOS Release 12.2(33)SXI onwards, authentication control-direction for more detail.
HostMode	Indicates whether the host-mode is single-host or multi-host, and effective from Cisco IOS Release 12.2(33)SXI onwards, multi-auth or multi-domain as well. See 'dot1x host-mode', or effective from Cisco IOS Release 12.2(33)SXI onwards, 'authentication host-mode' for more detail.
QuietPeriod	If authentication fails for a client, the authentication gets restarted after the quiet period shown in seconds.
ServerTimeout	Timeout that has been set for RADIUS retries. If an 802.1X packet is sent to the server and the server does not send a response, the packet will be sent again after the number of seconds that are shown.
SuppTimeout	Time that has been set for supplicant (client PC) retries. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the number of seconds that are shown.

Field	Description
ReAuthMax	The maximum amount of time in seconds after which an automatic reauthentication of a client PC is initiated.
MaxReq	Maximum number of times that the router sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client PC before concluding that the client PC does not support 802.1X.
TxPeriod	Timeout for supplicant retries, that is the timeout for EAP Identity Requests. See 'dot1x timeout tx-period' for more detail.
Supplicant	MAC address of the client PC or any 802.1X client.
Session ID	The ID of the network session.
Auth SM State	Describes the state of the client PC as either AUTHENTICATED or UNAUTHENTICATED.
Auth BEND SM State	The state of the IEEE 802.1X authenticator backend state machine.

Related Commands

Command	Description
clear dot1x	Clears 802.1X interface information.
debug dot1x	Displays 802.1X debugging information.
dot1x default	Resets the global 802.1X parameters to their default values.
identity profile	Creates an identity profile.
show authentication sessions	Displays information about current Authentication Manager sessions.

show dot1x (EtherSwitch)

To display the 802.1X statistics, administrative status, and operational status for the Ethernet switch network module or for the specified interface, use the **show dot1x** command in privileged EXEC mode.

show dot1x [statistics] [**interface interface-type interface-number**]

Syntax Description

statistics	(Optional) Displays 802.1X statistics.
interface *interface-type interface-number*	(Optional) Specifies the slot and port number of the interface to reauthenticate.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

If you do not specify an interface, global parameters and a summary appear. If you specify an interface, details for that interface appear.

If you specify an interface with the **statistics** keyword, statistics appear for all physical ports.

Examples

The following is sample output from the **show dot1x** command:

```
Router# show dot1x
Global 802.1X Parameters
    reauth-enabled               no
    reauth-period              3600
    quiet-period                 60
    tx-period                    30
    supp-timeout                 30
    server-timeout               30
    reauth-max                    2
    max-req                       2
802.1X Port Summary
    Port Name               Status      Mode                Authorized
    Gi0/1                   disabled    n/a                 n/a
    Gi0/2                   enabled     Auto (negotiate)    no
```

```
    802.1X Port Details
    802.1X is disabled on GigabitEthernet0/1
802.1X is enabled on GigabitEthernet0/2
      Status               Unauthorized
      Port-control         Auto
      Supplicant           0060.b0f8.fbfb
      Multiple Hosts       Disallowed
      Current Identifier   2
      Authenticator State Machine
        State              AUTHENTICATING
        Reauth Count       1
      Backend State Machine
        State              RESPONSE
        Request Count      0
        Identifier (Server) 2
      Reauthentication State Machine
        State              INITIALIZE
```

The table below describes the significant fields shown in the display.

Table 4: show dot1x Field Descriptions

Field	Description
reauth-enabled	Periodic reauthentication of client PCs on the interface has been enabled or disabled.
reauth-period	Time, in seconds, after which an automatic reauthentication will be initiated.
quiet-period	After authentication fails for a client, the authentication gets restarted after this quiet period shown in seconds.
tx-period	Time, in seconds, that the device waits for a response from a client to an Extensible Authentication Protocol (EAP) request or identity frame before retransmitting the request.
supp-timeout	Time, in seconds, that has been set for supplicant (client PC) retries. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the number of seconds that are shown.
server-timeout	Timeout, in seconds, that has been set for RADIUS retries. If an 802.1X packet is sent to the server and the server does not send a response, the packet will be sent again after the number of seconds that are shown.
reauth-max	The maximum number of times that the device tries to authenticate the client without receiving any response before the switch resets the port and restarts the authentication process.

Field	Description
max-req	Maximum number of times that the router sends an EAP request/identity frame (assuming that no response is received) to the client PC before concluding that the client PC does not support 802.1X.
Port Name	Interface type and slot/port numbers.
Status	Displays the 802.1X status of the port as either enabled or disabled.
Mode	Operational status of the port: • Auto--The port control value has been configured to be Force-unauthorized but the port has not changed to that state. • n/a--802.1X is disabled.
Authorized	Authorization state of the port.
Status	Status of the port (authorized or unauthorized). The status of a port appears as authorized if the **dot1x port-control** interface configuration command is set to **auto**, and authentication was successful.
Port-control	Setting of the **dot1x port-control** interface configuration command. The port control value is one of the following: • Auto--The authentication status of the client PC is being determined by the authentication process. • Force-authorize--All the client PCs on the interface are being authorized. • Force-unauthorized--All the client PCs on the interface are being unauthorized.
Supplicant	Ethernet MAC address of the client, if one exists. If the device has not discovered the client, this field displays *Not set* .
Multiple Hosts	Setting of the **dot1x multiple-hosts** interface configuration command (allowed or disallowed).

Field	Description
Current Identifier	Each exchange between the device and the client includes an identifier, which matches requests with responses. This number is incremented with each exchange and can be reset by the authentication server. **Note** This field and the remaining fields in the output show internal state information. For a detailed description of these state machines and their settings, refer to the IEEE 802.1X standard.

The following is sample output from the **show dot1x interface gigabitethernet0/2** privileged EXEC command. The table below describes the fields in the output.

```
Router# show dot1x interface gigabitethernet0/2
802.1X is enabled on GigabitEthernet0/2
  Status                Authorized
  Port-control          Auto
  Supplicant            0060.b0f8.fbfb
  Multiple Hosts        Disallowed
  Current Identifier    3
  Authenticator State Machine
    State               AUTHENTICATED
    Reauth Count        0
  Backend State Machine
    State               IDLE
    Request Count       0
    Identifier (Server) 2
Reauthentication State Machine
    State               INITIALIZE
```

The following is sample output from the **show dot1x statistics interface gigiabitethernet0/1** command. The table below describes the fields in the example.

```
Router# show dot1x statistics interface gigabitethernet0/1
GigabitEthernet0/1
    Rx: EAPOL     EAPOL     EAPOL     EAPOL     EAP       EAP       EAP
        Start     Logoff    Invalid   Total     Resp/Id   Resp/Oth  LenError
        0         0         0         21        0         0         0
        Last      Last
        EAPOLVer  EAPOLSrc
        1         0002.4b29.2a03
    Tx: EAPOL     EAP       EAP
        Total     Req/Id    Req/Oth
        622       445       0
```

Table 5: show dot1x statistics Field Descriptions

Field	Description
Rx EAPOL Start	Number of valid EAPOL-start frames that have been received. **Note** EAPOL = Extensible Authentication Protocol over LAN

Field	Description
Rx EAPOL Logoff	Number of EAPOL-logoff frames that have been received.
Rx EAPOL Invalid	Number of EAPOL frames that have been received and have an unrecognized frame type.
Rx EAPOL Total	Number of valid EAPOL frames of any type that have been received.
Rx EAP Resp/ID	Number of EAP-response/identity frames that have been received.
Rx EAP Resp/Oth	Number of valid EAP-response frames (other than response/identity frames) that have been received.
Rx EAP LenError	Number of EAPOL frames that have been received in which the packet body length field is invalid.
Last EAPOLVer	Protocol version number carried in the most recently received EAPOL frame.
LAST EAPOLSrc	Source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	Number of EAPOL frames of any type that have been sent.
Tx EAP Req/Id	Number of EAP-request/identity frames that have been sent.
Tx EAP Req/Oth	Number of EAP-request frames (other than request/identity frames) that have been sent.

Related Commands

Command	Description
dot1x default	Resets the global 802.1X parameters to their default values.

show dss log

To display the invalidation routes for the DSS range on the NetFlow table in the EXEC command mode, use the **show dss log** command.

show dss log {**ip**| **ipv6**}

Syntax Description

ip	Displays the range-invalidation profile for the DSS IP.
ipv6	Displays the range-invalidation profile for the DSS IPv6.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to support the **ipv6** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported in Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Whenever an IPv6 entry is deleted from the routing table, a message is sent to the switch processor to remove the entries that are associated to that network. Several IPv6 prefixes are collapsed to the less specific one if too many invalidations occur in a short period of time.

Examples

This example shows how to display the range-invalidation profile for the DSS IP:

```
Router# show dss log ip
22:50:18.551  prefix 172.20.52.18 mask 172.20.52.18
22:50:20.059  prefix 127.0.0.0 mask 255.0.0.0
22:51:48.767  prefix 172.20.52.18 mask 172.20.52.18
22:51:52.651  prefix 0.0.0.0 mask 0.0.0.0
22:53:02.651  prefix 0.0.0.0 mask 0.0.0.0
22:53:19.651  prefix 0.0.0.0 mask 0.0.0.0
Router#
```

show eap registrations

To display Extensible Authentication Protocol (EAP) registration information, use the **show eap registrations** command in privileged EXEC mode.

show eap registrations [**method**| **transport**]

Syntax Description

method	(Optional) Displays information about EAP method registrations only.
transport	(Optional) Displays information about EAP transport registrations only.

Command Default

If a keyword is not used, information is displayed for all lower layers used by EAP and for the methods that are registered with the EAP framework.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

This command is used to check which EAP methods are enabled on a router.

Examples

The following is an example of output from the show eap registrations command:

```
Router# show eap registrations
Registered EAP Methods:
Method Type Name
4 Peer MD5
Registered EAP Lower Layers:
Handle Type Name
2 Authenticator Dot1x-Authenticator
1 Authenticator MAB
```

The following is an example of output from the show eap registrations command using the transport keyword:

```
Router# show eap registrations transport
Registered EAP Lower Layers:
Handle Type Name
2 Authenticator Dot1x-Authenticator
```

The output fields are self-explanatory.

Related Commands

Command	Description
clear eap	Clears EAP session information for the switch or specified port.

show eap sessions

To display active Extensible Authentication Protocol (EAP) session information, use the **show eap sessions** command in privileged EXEC mode.

show eap sessions [**credentials** *credentials-name*| **interface** *interface-name*| **method** *method-name*| **transport** *transport-name*]

Syntax Description

credentials *credentials-name*	(Optional) Displays information about the specified credentials profile.
interface *interface-name*	(Optional) Displays information, such as type, module, and port number, about sessions that are associated with the specified interface.
method *method-name*	(Optional) Displays information about sessions that are associated with the specified EAP method.
transport *transport-name*	(Optional) Displays information about sessions that are associated with the specified lower layer.

Command Default

All active EAP sessions are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

The command output can be filtered using any of the optional keywords, singly or in combination.

Examples

The following is an example of output from the show eap sessions command:

```
Router# show eap sessions
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/1
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0x5200000A Credentials profile: None
```

```
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/2
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0xA800000B Credentials profile: None
Lower layer context ID: 0x0D000005 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
.
.
.
```

The following is an example of output from the show eap sessions interface command:

```
Router# show eap sessions interface gigabitethernet1/0/1
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/1
Current method: None Method state: Uninitialised
Retransmission count: 1 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 13s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
```

The fields in the above output are self-explanatory.

Related Commands

Command	Description
clear eap sessions	Clears EAP session information for the switch or for the specified port.

show eou

To display information about Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) global values or EAPoUDP session cache entries, use the **show eou** command in privileged EXEC mode.

show eou {**all**| **authentication** {**clientless**| **eap**| **static**}| **interface** *interface-type*| **ip** *ip-address*| **mac** *mac-address*| **posturetoken** *name*} [{**begin**| **exclude**| **include**} *expression*]

Syntax Description

all	Displays EAPoUDP information about all clients.
authentication	Authentication type.
clientless	Authentication type is clientless, that is, the endpoint system is not running Cisco Trust Agent (CTA) software.
eap	Authentication type is EAP.
static	Authentication type is statically configured.
interface	Provides information about the interface.
interface-type	Type of interface (see the table below for the interface types that may be shown).
ip	Specifies an IP address.
ip-address	IP address of the client device.
mac	Specifies a MAC address.
mac-address	The 48-bit address of the client device.
posturetoken	Displays information about a posture token name.
name	Name of the posture token.
begin	(Optional) Display begins with the line that matches the *expression* argument.
exclude	(Optional) Display excludes lines that match the *expression*argument.
include	(Optional) Display includes lines that match the specified *expression* argument.

expression	(Optional) Expression in the output to use as a reference point.

Command Default

All global EAPoUDP global values are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(25)SED	This command was integrated into Cisco IOS Release 12.2(25)SED.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The output of this command was enhanced to display information about whether the session is using the AAA timeout policy.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear.

Expressions are case sensitive. For example, if you enter "**exclude output**," the lines that contain "output" are not displayed, but the lines that contain "Output" appear.

The table below lists the interface types that may be used for the *interface-type* argument.

Table 6: Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface

Interface Type	Description
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicase Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following output displays information about a global EAPoUDP configuration. The default values can be changed or customized using the **eou default**, **eou max-retry**, **eou revalidate**, or **eou timeout** commands, depending on whether you configure them globally or on a specific interface.

```
Router# show eou
Global EAPoUDP Configuration
----------------------------
EAPoUDP Version     = 1
EAPoUDP Port        = 0x5566
Clientless Hosts    = Disabled
IP Station ID       = Disabled
Revalidation        = Enabled
Revalidation Period = 36000 Seconds
ReTransmit Period   = 3 Seconds
StatusQuery Period  = 300 Seconds
Hold Period         = 180 Seconds
AAA Timeout         = 60 Seconds
Max Retries         = 3
EAPoUDP Logging     = Disabled
Clientless Host Username = clientless
Clientless Host Password = clientless
Interface Specific EAPoUDP Configurations
------------------------------------------
Interface Ethernet2/1
```

No interface specific configuration

```
The following output displays information about a global EAPoUDP configuration that includes
 a NAC Auth Fail Open policy for use when the AAA server is unavailable:
Router# show eou ip 10.0.0.1
Address : 10.0.0.1
MAC Address : 0001.027c.f364
Interface : Vlan333
AuthType : AAA DOWN
AAA Down policy : rule_policy
Audit Session ID : 00000000011C11830000000311000001
PostureToken : -------
Age(min) : 0
URL Redirect : NO URL REDIRECT
URL Redirect ACL : NO URL REDIRECT ACL
ACL Name : rule_acl
Tag Name : NO TAG NAME
User Name : UNKNOWN USER
Revalidation Period : 500 Seconds
Status Query Period : 300 Seconds
Current State : AAA DOWN
```

The table below describes the significant fields shown in the display

Table 7: show eou Field Descriptions

Field	Description
EAPoUDP Version	EAPoUDP protocol version.
EAPoUDP Port	EAPoUDP port number.
Clientless Hosts	Clientless hosts are enabled or disabled.
IP Station ID	Specifies whether the IP address is allowed in the AAA station-id field. By default, it is disabled.
Revalidation	Revalidation is enabled or disabled.
Revalidation Period	Specifies whether revalidation of hosts is enabled. By default, it is disabled.
ReTransmit Period	Specifies the EAPoUDP packet retransmission interval. The default is 3 seconds.
StatusQuery Period	Specifies the EAPoUDP status query interval for validated hosts. The default is 300 seconds.
Hold Period	Hold period following a failed authentication.
AAA Timeout	AAA timeout period.
Max Retries	Maximum number of allowable retransmissions.
EAPoUDP Logging	Logging is enabled or disabled.

Field	Description
AAA Down policy	Name of policy to be applied when the AAA server is unreachable. (This is the NAC Auth Fail Open policy.)

Related Commands

Command	Description
eou default	Sets global EAPoUDP parameters to the default values.
eou max-retry	Sets the number of maximum retry attempts for EAPoUDP.
eou rate-limit	Sets the number of simultaneous posture validations for EAPoUDP.
eou timeout	Sets the EAPoUDP timeout values.

show epm session

To display information about Enforcement Policy Module (EPM) sessions, use the **show epm session**command in privileged EXEC mode.

show epm session {**interface** *type number*| **ip** {*ip-address* [**client** *client-type*]| **all**}| **mac** {*mac-address* [**client** *client-type*]| **all**}| **summary**}

Syntax Description

interface	Displays interface based session information.
type	Interface type.
number	Interface number.
ip	Displays information specifically for an IP address.
ip-address	IP address for the session.
client	(Optional) Specifies information about the type of client.
client-type	(Optional) Type of client. Values are **cts**, **dot1x**, **eapoudp**, **mab**, and **proxy**.
mac	Displays MAC address based session information.
mac-address	MAC address of the client.
all	Displays information for all sessions.
summary	Displays summary of session information such as IP address, MAC address, and so on for all the active sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2. The **all** keyword was added, and, **cts**, **dot1x**, and **mab** values for the *client-type* argument were added.

Examples

The following output shows information specifically for MAC address 0001.027c.f380:

```
Router#
show epm session mac 0001.027c.f380 client dot1x
Admission feature       : DOT1X
AAA Policies            :
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-459b9870
SGT                     : 1357-BAD123456789
```

The following output shows information specifically for IP address 10.9.0.1:

```
Router# show epm session ip 10.9.0.1
Admission feature       : AUTHPROXY
AAA Policies            :
Input Service Policy    : epm-pol-map
Proxy ACL               : permit udp any any
Proxy ACL               : deny icmp any any
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-472594af
Admission feature       : EAPOUDP
AAA Policies            :
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-459b9870
Proxy ACL               : permit udp any any
Proxy ACL               : permit icmp any any
Proxy ACL               : permit tcp an
Admission feature       : DOT1X
AAA Policies            :
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-459b9870
SGT                     : 1357-BAD123456789
```

The following example shows summary information for all sessions:

```
Router# show epm session summary
EPM Session Information
-------------------------
Total sessions seen so far : 5
Total active sessions      : 5
Interface              IP Address          MAC Address       Audit Session Id:
-------------------------------------------------------------------------------------------
GigabitEthernet7/2     209.165.200.225     0001.027c.f380    160000020000000000003A4EC
GigabitEthernet7/2     209.165.200.227     0001.027c.f380    160000020000000010003AD68
GigabitEthernet7/2     209.165.200.230     0001.027c.f380    160000020000000020003C110
GigabitEthernet7/2     209.165.200.235     0001.027c.f380    160000020000000030003D6BC
GigabitEthernet7/15    0.0.0.0             0030.6eb6.c69a    0904010C000000000002F6A4
```

The table below describes significant fields shown in the displays.

Table 8: show epm session ip Field Descriptions

Field	Description
Admission feature	Admission feature authentication proxy or Extensible Authentication Protocol over UDP (EOU) acting on the host.
AAA Policies	AAA policy information.
ACS ACL	Access control server (ACS) access control list (ACL).
SGT	Security group tag (SGT) value assigned to the host of that initiated the session.

Field	Description
Input Service Policy	Input service policy for the session.
Proxy ACL	Proxy access control list.
Total sessions seen so far	Total number of hosts connected to the Network Access Device (NAD) until now.
Total active sessions	Total number of active sessions.
Interface	Interface type and number.
IP Address	IP address of the host.
MAC Address	MAC address of the host.
Audit Session Id	Audit session ID.

show firewall vlan-group

To display secure virtual LANs (VLANs) attached to a secure group, use the **show firewall vlan-group** command in user EXEC or privileged EXEC mode.

show firewall vlan-group [*number*]

Syntax Description

number	(Optional) VLAN group number. The range is from 1 to 65535.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI1	This command was introduced.
12.2(33)SXJ	This command was modified. The command output was modified to display the VLAN groups created by both the Application Control Engine (ACE) and firewall.

Examples

The following is sample output from the **show firewall vlan-group** command:

```
Router# show firewall vlan-group

Display vlan-groups created by both ACE module and Firewall
Group    Created by      vlans
-----    ----------      -----
  142      Firewall      142
  200      Firewall      200-201
  360      Firewall      360-369
  380      Firewall      380-389
  500      Firewall      390-399
  660      Firewall      660-669
```

The table below describes the fields shown in the display.

Table 9: show firewall vlan-group Field Descriptions

Field	Description
Group	Group number to which the VLANs belong.

Field	Description
Created by	Indicates whether the VLAN groups are created by the ACE or the firewall.
vlans	VLAN ranges.

Related Commands

Command	Description
firewall	Specifies secure VLAN groups and attaches them to firewall modules.

show fm private-hosts

To display information about the Private Hosts feature manager, use the **show fm private-hosts** command in privileged EXEC mode.

show fm private-hosts {**all** | **interface** *type* / *num*}

Syntax Description

all	Displays the feature manager information for all of the interfaces that are configured for Private Hosts.
interface *type* / *num*	Displays the feature manager information for a specific interface. The slash (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example displays information about the Private Hosts feature manager:

```
Router# show fm private-hosts interface GigabitEthernet1/2
------------------------------------------------------------------------------
FM_FEATURE_PVT_HOST_INGRESS      i/f: Gi1/2      map name:
PVT_HOST_ISOLATED
==============================================================================
------------------------------------------------------------
MAC Seq. No: 10          Seq. Result : PVT_HOSTS_ACTION_DENY
------------------------------------------------------------
Indx - VMR index      T     - V(Value)M(Mask)R(Result)
EtTy - Ethernet Type  EtCo  - Ethernet Code
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+
 1    V 0000.0000.0000 0000.1111.4001    0 0
      M 0000.0000.0000 ffff.ffff.ffff    0 0
      TM_PERMIT_RESULT
 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT
------------------------------------------------------------
MAC Seq. No: 20          Seq. Result : PVT_HOSTS_ACTION_PERMIT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+
 1    V 0000.1111.4001 0000.0000.0000    0 0
      M ffff.ffff.ffff 0000.0000.0000    0 0
      TM_PERMIT_RESULT
```

```
 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT
------------------------------------------------------------
MAC Seq. No: 30          Seq. Result : PVT_HOSTS_ACTION_REDIRECT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+
 1    V ffff.ffff.ffff 0000.0000.0000    0 0
      M ffff.ffff.ffff 0000.0000.0000    0 0
      TM_PERMIT_RESULT
 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT
------------------------------------------------------------
MAC Seq. No: 40          Seq. Result : PVT_HOSTS_ACTION_PERMIT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+
 1    V 0100.5e00.0000 0000.0000.0000    0 0
      M ffff.ff80.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT
 2    V 3333.0000.0000 0000.0000.0000    0 0
      M ffff.0000.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT
 3    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT
------------------------------------------------------------
MAC Seq. No: 50          Seq. Result : PVT_HOSTS_ACTION_DENY
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+
 1    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT
 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT
Interfaces using this pvt host feature in ingress dir.:
------------------------------------------------
  Interfaces (I/E = Ingress/Egress)
```

Related Commands

Command	Description
private-hosts	Enables or configures the private host feature.
private-hosts mode	Sets the switchport mode.
show fm private-hosts	Displays the FM-related private hosts information.
show private-hosts configuration	Displays Private Hosts configuration information for the router.
show **private-hosts interface configuration**	Displays Private Hosts configuration information for individual interfaces.

show fpm package-group

Note Effective with Cisco IOS Release 15.2(4)M, the **show fpm package-group** command is not available in Cisco IOS software.

To display configuration information about flexible packet matching (FPM) package support, use the **show fpm package-group** command in user EXEC or privileged EXEC mode.

show fpm package-group [**control-plane**| **fpm-package-group**| **interface interface-name**]

Syntax Description

control-plane	(Optional) Displays FPM package group control plane information.
fpm-group-name	(Optional) Displays FPM group name information.
interface	(Optional) Displays FPM package group interface information.
interface-name	Name of the Interface for which you want to show the FPM package group information. See the table below for a list of valid interfaces.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

The table below displays valid interfaces that may be shown as the *interface-name* argument with the **interface** keyword.

Table 10: Interfaces That Can Be Shown

Interface	Description
ATM	ATM interface
Async	Asynchronous interface

Interface	Description
Auto-template	Auto-Template interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	CDMA Ix interface
CTunnel	CTunnel interface
Dialer	Dialer interface
FastEthernet	FastEthernet IEEE 802.3
Lex	Lex interface
LongReachEthernet	Long-Reach Ethernet interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Pos	Packet over SONET interface
Port-channel	Ethernet channel of interfaces
SSLVPN-VIF	Secure Socket Layer Virtual Private Network (SSLVPN) Virtual Interface
Serial	Serial
Tunnel	Tunnel interface
vif	Pragmatic General Multicast (PGM) multicast host interface
virtual-PPP	Virtual PPP interface
virtual-Template	Virtual template interface
virtual-TokenRing	Virtual TokenRing
vmi	Virtual Multipoint Interface

Examples

The following is sample output from the **show fpm package-group** command.

```
Router# show fpm package-group

 group name: cisco-fpm-packages
  auto-load
  fpm package: fpm-package-11
  fpm package: fpm-package-43
   package action: log
```

The table below describes the significant fields shown in the display.

Table 11: show fpm package-group Field Descriptions

Field	Description
Auto-load	Displays if automatic loading of FPM package support is configured.
FPM package	Displays the name of the FPM package loaded from the FPM-server.
Group name	Displays the protocol to connect to the FPM-server.
Package action	Displays the action taken when the FPM package is loaded.

Related Commands

Command	Description
show fpm package-info	Displays FPM package transfer configuration details.

show fpm package-info

Note Effective with Cisco IOS Release 15.2(4)M, the **show fpm package-info** command is not available in Cisco IOS software.

FPM server
To display information about fpm package transfer between an FPM server and a local server, use the **show fpm package-info** command in user EXEC or privileged EXEC mode.

show fpm package-info

Syntax Description

This command has no keywords or arguments.

Command Default

The command displays information about the transfer of fpm package groups from the FPM server to a local server.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Examples

The following is sample output from the **show fpm package-info** command.

```
Router# show fpm package-info
Router# show fpm package-info
 fpm package-info
  host 10.0.0.1
  remote-path bluebell/
  local-path flash:
  user cisco
  password 7 0101130A5D04141D245F5A1B0C0B57
  protocol tftp
  time-range weekly
```

The table below describes the significant fields shown in the display.

Table 12: show fpm package-info Field Descriptions

Field	Description
Host	Displays the download server address.

Field	Description
Local-path	Displays the location where packages are stored on the local router.
Password	Displays and encrypted password for the server.
Protocol	Displays the protocol to connect to the server.
Remote-path	Displays the file server name.
Time-range	Displays the interval between searches for fpm updates.
User	Displays the username on the server.

Related Commands

Command	Description
show fpm package-group	Displays fpm package matching support configuration details.

show fm raguard

To display the interfaces configured with router advertisement (RA) guard, use the **show fm raguard**command in privileged EXEC mode.

show fm raguard

Syntax Description

This command has no arguments or keywords.

Command Default

RA guard interface information is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.

Usage Guidelines

Use the **show fm raguard** command to verify information about interfaces that are configured with RA guard.

Examples

The following example enables the display of interfaces configured with IPv6 RA guard:

```
Router# show fm raguard
------------------------------------------------------------------------------
 IPV6 RA GUARD in Ingress direction is configured on following interfaces
==============================================================================
Interface: Port-channel23
Interface: GigabitEthernet4/6
```

The table below describes the significant fields shown in the display.

Table 13: show fm raguard Field Descriptions

Field	Description
IPV6 RA GUARD in Ingress direction is configured on following interfaces	Displays the interfaces configured with IPv6 RA guard.

show idmgr

To display information related to the Intelligent Services Gateway (ISG) session identity, use the **show idmgr** command in privileged EXEC mode.

show idmgr {[**memory detailed component** *substring*]| **service key session-handle** *session-handle* **service-key** *key-value*| **session key**| **aaa-unique-id** *aaa-unique-id-string*| **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*| **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number*| **session-guid** *session-guid*| **session-handle** *session-handle-string*| **session-id** *session-id-string*| **circuit-id** *circuit-id*| **pppoe-unique-id** *pppoe-id*| **statistics**}

Syntax Description

memory	Displays memory-usage information related to ID management.
detailed	(Optional) Displays detailed memory-usage information related to ID management.
component	(Optional) Displays information for the specified ID management component.
substring	(Optional) Substring to match the component name.
service key	Displays ID information for a specific service.
session-handle *session-handle-string*	Displays the unique identifier for a session.
service-key *key-value*	Displays ID information for a specific service.
session key	Displays ID information for a specific session and its related services.
aaa-unique-id *aaa-unique-id-string*	Displays the authentication, authorization, and accounting (AAA) unique ID for a specific session.
domainip-vrf ip-address *ip-address*	Displays the service-facing IP address for a specific session.
vrf-id *vrf-id*	Displays the VPN routing and forwarding (VRF) ID for the specific session.
nativeip-vrf ip-address *ip-address*	Displays the subscriber-facing IP address for a specific session.
portbundle ip *ip-address*	Displays the port bundle IP address for a specific session.
bundle *bundle-number*	Displays the bundle number for a specific session.

session-guid *session-guid*	Displays the global unique identifier for a session.
session-handle *session-handle-string*	Displays the session identifier for a specific session.
session-id *session-id-string*	Displays the session identifier used to construct the value for RADIUS attribute 44 (Acct-Session-ID).
circuit-id *circuit-id*	Displays the user session information in the ID Manager (IDMGR) database when you specify the unique circuit ID tag.
pppoe-**unique-id** *pppoe-id*	Displays the PPPoE unique key information in the ID Manager (IDMGR) database when you specify the unique PPPoE unique ID tag
statistics	Displays statistics related to storing and retrieving ID information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	The circuit-id keyword and *circuit-id*argument was added.

Examples

The following sample output for the **show idmgr** command displays information about the service called "service":

```
Router# show idmgr service key session-handle 48000002 service-key service
session-handle = 48000002
service-name = service
idmgr-svc-key = 4800000273657276696365
authen-status = authen
```

The following sample output for the **show idmgr** command displays information about a session and the service that is related to the session:

```
Router# show idmgr session key session-handle 48000002

session-handle = 48000002
aaa-unique-id = 00000002
authen-status = authen
username = user1
Service 1 information:
session-handle = 48000002
service-name = service
idmgr-svc-key = 4800000273657276696365
```

The following sample output for the **show idmgr** command displays information about the global unique identifier of a session:

```
Router# show idmgr session key session-guid 0202020100000000C
session-handle = 18000003
aaa-unique-id = 0000000C
authen-status = authen
interface = nas-port:0.0.0.0:2/0/0/42
authen-status = authen
username = FortyTwo
addr = 100.42.1.1
session-guid = 0202020100000000C
The following sample output for the show idmgr
 command displays information about the user session information in the ID Manager (IDMGR)
 database by specifying the unique circuit ID tag:
Router# show idmgr session key circuit-id Ethernet4/0.100:PPPoE-Tag-1
session-handle = AA000007
aaa-unique-id = 0000000E
circuit-id-tag = Ethernet4/0.100:PPPoE-Tag-1
interface = nas-port:0.0.0.0:0/1/1/100
authen-status = authen
username = user1@cisco.com
addr = 106.1.1.3
session-guid = 650101020000000E
The session hdl AA000007 in the record is valid
The session hdl AA000007 in the record is valid
No service record found
```

The table below describes the significant fields shown in the display.

Table 14: show idmgr Field Descriptions

Field	Description
session-handle	Unique identifier of the session.
service-name	Service name for this session.
idmgr-svc-key	The ID manager service key of this session.
authen-status	Indicates whether the session has been authenticated or unauthenticated.
aaa-unique-id	AAA unique ID of the session.
username	The username associated with this session.
interface	The interface details of this session.
addr	The IP address of this session.
session-guid	Global unique identifier of this session.

Related Commands

Command	Description
subscriber access pppoe unique-key circuit-id	Specifies a unique circuit ID tag for a PPPoE user session to be tapped on the router.

show interface virtual-access

To display virtual access interface information, use the **show interface virtual-access** command in user EXEC or privileged EXEC mode.

show interface virtual-access *interface-number* [**accounting**| **configuration**| **counters protocol status**| **crb**| **dampening**| **description**| **fair-queue**| **irb**| **mpls-exp**| **precedence**| **random-detect**| **rate-limit**| **stats**| **summary**| **switching**]

Syntax Description

interface-number	Virtual access interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
accounting	(Optional) Displays virtual access interface accounting information.
configuration	(Optional) Displays virtual access interface configuration information.
counters protocol status	(Optional) Displays information about the current status of protocol counters that are enabled.
crb	(Optional) Displays virtual access interface concurrent routing and bridging (CRB) information.
dampening	(Optional) Displays virtual access interface dampening information.
description	(Optional) Displays virtual access interface description.
fair-queue	(Optional) Displays virtual access interface weighted fair queueing (WFQ) information.
irb	(Optional) Displays virtual access interface integrated routing and bridging (IRB) information.
mpls-exp	(Optional) Displays virtual interface Multiprotocol Label Switching (MPLS) experimental accounting information.
precedence	(Optional) Displays virtual interface precedence accounting information.
random-detect	(Optional) Displays virtual interface Weighted Random Early Detection (WRED) information.

rate-limit	(Optional) Displays virtual interface rate-limit information.
stats	(Optional) Displays virtual interface packets and octets, in and out, by switching path.
summary	(Optional) Displays the virtual interface summary.
switching	(Optional) Displays virtual interface switching information.

Command Default

If no keyword is specified, general information about virtual access interfaces is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced in a release earlier than Cisco IOS Release 15.1(1)T.

Examples

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

```
Router# show interface virtual-access 1
Virtual-Access1 is up, line protocol is up
Hardware is Virtual Access interface
Description: ***Internally created by SSLVPN context c3***
Interface is unnumbered. Using address of Virtual-Access1 (0.0.0.0)
MTU 1406 bytes, BW 100000 Kbit/sec, DLY 100000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation SSL
SSL vaccess, cloned from Virtual-Template1
Vaccess status 0x4, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters 2d16h
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 24 bits/sec, 10 packets/sec
5 minute output rate 16 bits/sec, 10 packets/sec
100 packets input, 2000 bytes, 23 no buffer
Received 79 broadcasts, 30 runts, 20 giants, 29 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
12 packets output, 1100 bytes, 10 underruns
6 output errors, 5 collisions, 1 interface resets
9 unknown protocol drops
10 unknown protocol drops
29 output buffer failures, 10 output buffers swapped out
25 carrier transitions
```

The table below describes the significant fields shown in the display.

Table 15: show interface virtual-access Field Descriptions

Field	Description
Using address of Virtual-Access1	IP address of the virtual interface.
MTU	MTU, in bytes. Default: 1500.
BW	Bandwidth, in Kb/s.
DLY	Delay, in microseconds.
reliability	Reliability of the interface as a fraction of 255. Default: Calculated as an exponential average over five minutes. • 255/255 provides 100 percent reliability.
txload	Transmission load on an interface as a fraction of 255.
rxload	Receiver load on an interface as a fraction of 255.
Encapsulation	Data-link encapsulation.
SSL vaccess	Specifies Secure Socket Layer Virtual Private Network (SSL VPN) virtual access.
Vaccess status	Status of the virtual access.
ARP type	Type of Address Resolution Protocol (ARP).
ARP Timeout	Amount of time an entry remains in the ARP cache.
Input queue	Number of packets in the input queue.
Total output drops	Total number of packets dropped.
Queueing strategy	Theory followed to treat the packets in a queue.
Output queue	Number of packets in the output queue.
broadcasts	Total number of broadcast or multicast packets received.
runts	Total number of packets discarded due to the packet size being less than the minimum packet size (64 bytes).
giants	Total number of packets discarded due to the packet size exceeding the maximum packet size.

Field	Description
throttles	Total number of throttles.
input errors	Total number of errors that prevented the receipt of datagrams.
CRC	Mismatch generated by the cyclic redundancy checksum (CRC).
frame	Total number of packets received with a CRC error.
overrun	Total number of times data has not reached the serial receiver buffer because of the input rate is more than the receiver can handle.
ignored	Total number of packets ignored by the interface because of the scarcity of internal buffers.
abort	Total number of packets aborted.
output errors	Total number of errors that prevented the final transmission.
collisions	Total number of collisions encountered.
interface resets	Total number of times an interface has been completely reset.
output buffer failures	Total number of buffer failures.
carrier transitions	Interface transitions.

Related Commands

Command	Description
clear interface virtual-access	Clears the virtual access interface and frees the memory for other dial-in uses.

show ip access-lists

To display the contents of all current IP access lists, use the **show ip access-lists** command in user EXEC or privileged EXEC modes.

show ip access-lists [*access-list-number*| *access-list-number-expanded-range*| *access-list-name*| **dynamic** [*dynamic-access-list-name*]| **interface** *name number* [**in**| **out**]]

Syntax Description

access-list-number	(Optional) Number of the IP access list to display.
access-list-number-expanded-range	(Optional) Expanded range of the IP access list to display.
access-list-name	(Optional) Name of the IP access list to display.
dynamic *dynamic-access-list-name*	(Optional) Displays the specified dynamic IP access lists.
interface *name number*	(Optional) Displays the access list for the specified interface.
in	(Optional) Displays input interface statistics.
out	(Optional) Displays output interface statistics.

Command Default

All standard and expanded IP access lists are displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.3(7)T	The **dynamic** keyword was added.
12.4(6)T	The **interface** *name*and *number* keyword and argument pair was added. The **in** and **out** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was modified. Example output from the **dynamic** keyword was added.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. The output of this command was extended to display access lists that contain object groups.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The **show ip access-lists** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ip access-lists** command when all access lists are requested:

```
Router# show ip access-lists
Extended IP access list 101
   deny udp any any eq nntp
   permit tcp any any
   permit udp any any eq tftp
   permit icmp any any
   permit udp any any eq domain
```

The table below describes the significant fields shown in the display.

Table 16: show ip access-lists Field Descriptions

Field	Description
Extended IP access list	Extended IP access-list number.
deny	Packets to reject.
udp	User Datagram Protocol.
any	Source host or destination host.
eq	Packets on a given port number.
nntp	Network News Transport Protocol.
permit	Packets to forward.
tcp	Transmission Control Protocol.
tftp	Trivial File Transfer Protocol.
icmp	Internet Control Message Protocol.
domain	Domain name service.

The following is sample output from the **show ip access-lists** command when the name of a specific access list is requested:

```
Router# show ip access-lists Internetfilter
Extended IP access list Internetfilter
   permit tcp any 192.0.2.0 255.255.255.255 eq telnet
   deny tcp any any
   deny udp any 192.0.2.0 255.255.255.255 lt 1024
   deny ip any any log
```

The following is sample output from the **show ip access-lists** command when the name of a specific access list that contains an object group is requested:

```
Router# show ip access-lists my-ogacl-policy
Extended IP access list my-ogacl-policy
   10 permit object-group eng-service any any
```

The following sample output from the **show ip access-lists** command shows input statistics for Fast Ethernet interface 0/0:

```
Router#
 show ip access-lists interface FastEthernet0/0 in

Extended IP access list 150 in
   10 permit ip host 10.1.1.1 any
   30 permit ip host 10.2.2.2 any (15 matches)
```

The following is sample output from the **show ip access-lists** command using the **dynamic** keyword:

```
Router#
show ip access-lists dynamic CM_SF#1
Extended IP access list CM_SF#1
    10 permit udp any any eq 5060 (650 matches)
    20 permit tcp any any eq 5060
    30 permit udp any any dscp ef (806184 matches)
```

To check your configuration, use the **show run interfaces cable** command:

```
Router#
show run interfaces cable 0/1/0
Building configuration...
Current configuration : 144 bytes
!
interface cable-modem0/1/0
 ip address dhcp
 load-interval 30
 no keepalive
  service-flow primary upstream
   service-policy output llq
end
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.

Command	Description
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show object-group	Displays information about object groups that are configured.
show run interfaces cable	Displays statistics on the cable modem.

show ip admission

To display the network admission cache entries and information about web authentication sessions, use the **show ip admission** command in user EXEC or privileged EXEC mode.

Cisco IOS XE Release 3SE and Later Releases

show ip admission {**cache**| **statistics** [**brief**| **details**| **httpd**| **input-feature**]| **status** [**banners**| **custom-pages**| **httpd**| **parameter-map** [*parameter-map-name*]]| **watch-list**}

All Other Releases

show ip admission {**cache** [**consent**| **eapoudp**| **ip-addr** *ip-address*| **username** *username*]| **configuration**| **httpd**| **statistics**| [**brief**| **details**| **httpd**]| **status [httpd]**| **watch-list**}

Syntax Description

cache	Displays the current list of network admission entries.
statistics	Displays statistics for web authentication.
brief	(Optional) Displays a statistics summary for web authentication.
details	(Optional) Displays detailed statistics for web authentication.
httpd	(Optional) Displays information about web authentication HTTP processes
input-feature	Displays statistics about web authentication packets.
status	Displays status information about configured web authentication features including banners, custom pages, HTTP processes, and parameter maps.
banners	Displays information about configured banners for web authentication.
custom-pages	Displays information about custom pages configured for web authentication. Custom files are read into a local cache and served from the cache. A background process periodically checks if the files need to be re-cached.
parameter-map *parameter-map-name*	Displays information about configured banners and custom pages for all parameter maps or only for the specified parameter map.
watch-list	Displays the list of IP addresses in the watch list.

consent	(Optional) Displays the consent web page cache entries.
eapoudp	(Optional) Displays the Extensible Authentication Protocol over UDP (EAPoUDP) network admission cache entries. Includes the host IP addresses, session timeout, and posture state.
ip-addr *ip-address*	(Optional) Displays information for a client IP address.
username *username*	(Optional) Display information for a client username.
configuration	(Optional) Displays the NAC configuration. **Note** This keyword is not supported in Cisco IOS XE Release 3.2SE and later releases. Use the **show running-config all** command to see the running web authentication configuration and the commands configured with default parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was modified. The output of this command was enhanced to display whether the AAA timeout policy is configured.
12.4(15)T	This command was modified. The **consent** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.3(1)T	This command was modified. The **statistics**, **brief**, **details**, **httpd**, and **status** keywords were added.
Cisco IOS XE Release 3.2SE	This command was modified. The **input-feature**, **banners**, **custom-pages**, and **parameter-map** keywords were added. The **configuration** keyword was removed.

Usage Guidelines

Use the **show ip admission** command to display information about network admission entries and information about web authentication sessions.

Examples

The following is sample output from the **show ip admission cache** command:

```
Device# show ip admission cache

Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 1
 Client MAC 5cf3.fc25.7e3d Client IP 1.150.128.2 IPv6 :: Port 0, State INIT, Method Webauth
```

The following is sample output from the **show ip admission statistics** command:

```
Device# show ip admission statistics

Webauth input-feature statistics:
                                                        IPv4          IPv6
  Total packets received                                46            0
    Delivered to TCP                                    46            0
    Forwarded                                           0             0
    Dropped                                             0             0
    TCP new connection limit reached                    0             0

Webauth HTTPd statistics:

  HTTPd process 1
    Intercepted HTTP requests:                          8
    IO Read events:                                     9
    Received HTTP messages:                             7
    IO write events:                                    11
    Sent HTTP replies:                                  7
    IO AAA messages:                                    4
    SSL OK:                                             0
    SSL Read would block:                               0
    SSL Write would block:                              0
    HTTPd process scheduled count:                      23
```

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

```
Device# show ip admission status

IP admission status:
  Enabled interfaces            1
  Total sessions                1
  Init sessions                 1     Max init sessions allowed     100
    Limit reached               0     Hi watermark                  1
  TCP half-open connections     0     Hi watermark                  0
  TCP new connections           0     Hi watermark                  0
  TCP half-open + new           0     Hi watermark                  0
  HTTPD1 Contexts               0     Hi watermark                  1

  Parameter Map: Global
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Custom Pages
      Custom pages not configured
    Banner
      Type: text
        Banner                  " <H2>Login Page Banner</H2> "
        Html                    " <H2>Login Page Banner</H2> "
        Length                  48

  Parameter Map: PMAP_CONSENT
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBCONSENT
    Custom Pages
      Custom pages not configured
```

```
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_FLASH
    Custom Pages
      Type: "login"
        File                    flash:webauth_login.html
        File status             Ok - File cached
        File mod time           2012-07-20T02:29:36.000Z
        File needs re-cached    No
        Cache                   0x3AEE1E1C
        Cache len               246582
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "success"
        File                    flash:webauth_success.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:57:28.000Z
        File needs re-cached    No
        Cache                   0x3A529B3C
        Cache len               70
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "failure"
        File                    flash:webauth_fail.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:49.000Z
        File needs re-cached    No
        Cache                   0x3A5BEBC4
        Cache len               67
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "login expired"
        File                    flash:webauth_expire.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:25.000Z
        File needs re-cached    No
        Cache                   0x3AA20090
        Cache len               69
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_EXTERNAL
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured
```

The following is sample output from the **show ip admission status banners** command for a banner configured with the **banner text** command:

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Type: text
      Banner                    " <H2>Login Page Banner</H2> "
      Html                      " <H2>Login Page Banner</H2> "
      Length                    48
```

The following is sample output from the **show ip admission status banners** command for a banner configured with the **banner file** command:

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured
```

```
  Parameter Map: PMAP_WEBAUTH
    Type: file
      Banner                    <h2>Cisco Systems</h2>
<h3>Webauth Banner from file</h3>

      Length                    60
      File                      flash:webauth_banner1.html
      File status               Ok - File cached
      File mod time             2012-07-24T07:07:09.000Z
      File needs re-cached      No
      Cache                     0x3AF6CEE4
      Cache len                 60
      Cache time                2012-09-19T10:13:59.000Z
      Cache access              0 reads, 1 write
```

The following is sample output from the **show ip admission status custom pages** command:

```
Device# show ip admission status custom pages

IP admission status:
  Parameter Map:  Global
    Custom pages not configured
  Parameter Map:  PMAP_WEBAUTH
    Type: "login"
      File                      flash:webauth_login.html
      File status               Ok - File cached
      File mod time             2012-07-20T02:29:36.000Z
      File needs re-cached      No
      Cache                     0x3B0DCEB4
      Cache len                 246582
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
    Type: "success"
      File                      flash:webauth_success.html
      File status               Ok - File cached
      File mod time             2012-02-21T06:57:28.000Z
      File needs re-cached      No
      Cache                     0x3A2E9090
      Cache len                 70
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
    Type: "failure"
      File                      flash:webauth_fail.html
      File status               Ok - File cached
      File mod time             2012-02-21T06:55:49.000Z
      File needs re-cached      No
      Cache                     0x3AF6D1A4
      Cache len                 67
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
    Type: "login expired"
      File                      flash:webauth_expire.html
      File status               Ok - File cached
      File mod time             2012-02-21T06:55:25.000Z
      File needs re-cached      No
      Cache                     0x3A2E8284
      Cache len                 69
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
  Parameter Map:  PMAP_CONSENT
    Custom pages not configured
```

The following table describes the significant fields shown in the above display.

Table 17: show ip admission Field Descriptions

File mod time	Time stamp when the file was changed on the file system.
Cache time	Time stamp when the file was last read into cache.

The following output displays all the IP admission control rules that are configured on a router:

```
Device# show ip admission configuration

Authentication Proxy Banner not configured
Consent Banner is not configured
Authentication Proxy webpage
        Login page              : flash:test1.htm
        Success page            : flash:test1.htm
        Fail page               : flash:test1.htm
        Login Expire page       : flash:test1.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 5 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

The following output displays the host IP addresses, the session timeout, and the posture states. If the posture statue is POSTURE ESTAB, the host validation was successful.

```
Device# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

The fields in the displays are self-explanatory.

Related Commands

Command	Description
banner (parameter-map webauth)	Displays a banner on the web-authentication login web page.
clear ip admission cache	Clears IP admission cache entries from the router.
custom-page	Displays custom web pages during web authentication login.
ip admission name	Creates a Layer 3 network admission control rule.

show ip audit configuration

To display additional configuration information, including default values that may not be displayed using the **show running-config**command, use the **show ip audit configuration** command in EXEC mode.

show ip audit configuration

Syntax Description

This command has no argument or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip audit configuration** EXEC command to display additional configuration information, including default values that may not be displayed using the **show running-config** command.

Examples

The following example displays the output of the **show ip audit configuration** command:

```
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)

Audit Rule Configuration
 Audit name AUDIT.1
    info actions alarm
```

Related Commands

Command	Description
clear ip audit statistics	Resets statistics on packets analyzed and alarms sent.

show ip audit interface

To display the interface configuration, use the **show ip audit interface** command in EXEC mode.

show ip audit interface

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip audit interface** EXEC command to display the interface configuration.

Examples

The following example displays the output of the **show ip audit interface** command:

```
Interface Configuration
 Interface Ethernet0
  Inbound IDS audit rule is AUDIT.1
    info actions alarm
  Outgoing IDS audit rule is not set
 Interface Ethernet1
  Inbound IDS audit rule is AUDIT.1
    info actions alarm
  Outgoing IDS audit rule is AUDIT.1
    info actions alarm
```

show ip audit statistics

To display the number of packets audited and the number of alarms sent, among other information, use the **show ip audit statistics** command in EXEC mode.

show ip audit statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip audit statistics** EXEC command to display the number of packets audited and the number of alarms sent, among other information.

Examples

The following displays the output of the **show ip audit statistics** command:

```
Signature audit statistics [process switch:fast switch]
  signature 2000 packets audited: [0:2]
  signature 2001 packets audited: [9:9]
  signature 2004 packets audited: [0:2]
  signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
Session creations since subsystem startup or last reset 11
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:0]
Last session created 19:18:27
Last statistic reset never

HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0
```

Related Commands

Command	Description
clear ip audit statistics	Resets statistics on packets analyzed and alarms sent.

show ip auth-proxy

To display the authentication proxy entries or the authentication proxy configuration, use the **show ip auth-proxy** command in privileged EXEC mode.

show ip auth-proxy {**cache**| **configuration**| **httpd**| **statistics**| [**brief**| **details**| **httpd**]| **watch-list**}

Syntax Description

cache	Displays the current list of the authentication proxy entries.
configuration	Displays the authentication proxy configuration. **Note** This keyword is not available in Cisco IOS XE Release 3.2SE and later releases. Use the **show running-config all** command to see the running web authentication configuration and the commands configured with default parameters.
httpd	Displays information about web authentication HTTP processes
statistics	Displays statistics for web authentication.
brief	(Optional) Displays a statistics summary for web authentication.
details	(Optional) Displays detailed statistics for web authentication.
watch-list	Displays the list of users on the watch list.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
15.3(1)T	This command was modified. The **httpd**, **statistics**, **brief**, and **details** keywords were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE. The **configuration** keyword was removed.

Usage Guidelines

Use the **show ip auth-proxy** to display either the authentication proxy entries or the running authentication proxy configuration. Use the **cache** keyword to list the host IP address, the source port number, the timeout value for the authentication proxy, and the state for connections using authentication proxy. If authentication proxy state is HTTP_ESTAB, the user authentication was successful.

Use the **configuration** keyword to display all authentication proxy rules configured on the device.

Examples

The following example shows sample output from the **show ip auth-proxy cache** command after one user authentication using the authentication proxy:

```
Device# show ip auth-proxy cache
Authentication Proxy Cache
Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

The following example shows how the **show ip auth-proxy configuration** command displays the information about the authentication proxy rule named pxy. The global idle timeout value is 60 minutes. The idle timeouts value for this named rule is 30 minutes. No host list is specified in the rule, meaning that all connection initiating HTTP traffic at the interface is subject to the authentication proxy rule.

```
Device# show ip auth-proxy configuration
Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 30 minutes
```

Related Commands

Command	Description
clear ip auth-proxy cache	Clears authentication proxy entries from the device.
ip auth-proxy	Sets the authentication proxy idle timeout value (the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity).
ip auth-proxy (interface configuration)	Applies an authentication proxy rule at a firewall interface.
ip auth-proxy name	Creates an authentication proxy rule.

show ip auth-proxy watch-list

To display the information about the authentication proxy watch list in the EXEC command mode, use the **show ip auth-proxy watch-list** command.

show ip auth-proxy watch-list

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Examples

This example shows how to display the information about the authentication proxy watch list:

```
Router# show ip auth-proxy watch-list
Authentication Proxy Watch-list is enabled
Watch-list expiry timeout is 2 minutes
Total number of watch-list entries: 3
 Source IP       Type         Violation-count
 10.0.0.2        MAX_RETRY    MAX_LIMIT
 10.0.0.3        TCP_NO_DATA  MAX_LIMIT
 10.255.255.255 CFGED        N/A
Total number of watch-listed users: 3
Router#
```

Related Commands

Command	Description
clear ip auth-proxy watch-list	Deletes a single watch-list entry or all watch-list entries.
ip auth-proxy max-login-attempts	Limits the number of login attempts at a firewall interface.

Command	Description
ip auth-proxy watch-list	Enables and configures an authentication proxy watch list.

show ip bgp labels

To display information about Multiprotocol Label Switching (MPLS) labels from the external Border Gateway Protocol (eBGP) route table, use the **show ip bgp labels** command in privileged EXEC mode.

show ip bgp labels

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to display eBGP labels associated with an Autonomous System Boundary Router (ASBR).

This command displays labels for BGP routes in the default table only. To display labels in the Virtual Private Network (VPN) routing and forwarding (VRF) tables, use the **show ip bgp vpnv4** {**all** | **vrf** *vrf-name*} command with the optional **labels** keyword.

Examples

The following example shows output for an ASBR using BGP as a label distribution protocol:

```
Router# show ip bgp labels
Network          Next Hop         In Label/Out Label
10.3.0.0/16       0.0.0.0          imp-null/exp-null
10.15.15.15/32   10.15.15.15      18/exp-null
10.16.16.16/32   0.0.0.0          imp-null/exp-null
10.17.17.17/32   10.0.0.1         20/exp-null
```

```
10.18.18.18/32   10.0.0.1         24/31
10.18.18.18/32   10.0.0.1         24/33
```

The table below describes the significant fields shown in the display.

Table 18: show ip bgp labels Field Descriptions

Field	Description
Network	Displays the network address from the eBGP table.
Next Hop	Specifies the eBGP next hop address.
In Label	Displays the label (if any) assigned by this router.
Out Label	Displays the label assigned by the BGP next hop router.

Related Commands

Command	Description
show ip bgp vpnv4	Displays VPN address information from the BGP table.

show ip device tracking

To display information about entries in the IP device tracking table, use the **show ip device tracking** command in privileged EXEC mode.

show ip device tracking {**all count**| **interface** *type-of-interface*| **ip** *ip-address*| **mac** *mac-address*}

Syntax Description

all count	Displays a count of all IP tracking host entries.
interface *type-of-interface*	Displays interface information. See the table below for a list of valid interfaces.
ip *ip-address*	Displays the IP address of the client.
mac *mac-address*	Displays the 48-bit hardware MAC address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2SX	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The table below displays valid interfaces that may be shown as the *type-of-interface*argument with the **interface**keyword.

Table 19: Interfaces That Can Be Tracked

Interface	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	CDMA Ix interface
CTunnel	CTunnel interface
Dialer	Dialer interface
FastEthernet	FastEthernet IEEE 802.3

Interface	Description
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle intrface
Multilink	Multilink-group interface
Null	Null interface
Port-channel	Ethernet channel of interfaces
Serial	Serial
Tunnel	Tunnel interface
vif	Pragmatic General Multicast (PGM) multicast host interface
virtual	Virtual interface
virtual-PPP	Virtual PPP interface
virtual-Template	Virtual template interface
virtual-TokenRing	Virtual TokenRing
XTagATM	Extended Tag ATM interface

Examples

The following example shows that all host entries are to be tracked:

```
Router# show ip device tracking all count
IP Device Tracking = Enabled
Probe Count: 2
Probe Interval: 10
```

The fields in the above display are self-explanatory.

show ip inspect

To display Context-Based Access Control (CBAC) configuration and session information, use the **show ip inspect**command in privileged EXEC mode.

ACL Bypass Statistics Syntax

show ip inspect {**name** *inspection-name*| **config**| **interfaces**| **sessions [detail]**| **statistics [reset]**| **all**| **sis [detail]**| **tech-support [reset]**} [**vrf** *vrf-name*]

Firewall MIB Statistics Syntax

show ip inspect mib connection-statistics {**global**| **l4-protocol** {**all**| **icmp**| **tcp**| **udp**}| **l7-protocol** [*protocol-type*]| **policy** *policy-name* **interface** [*interface-type interface-number*] **l4-protocol** {**all**| **icmp**| **tcp**| **udp**}| **l7-protocol** [*protocol-type*]}

Syntax Description

name *inspection-name*	Displays the configured inspection rule with the name *inspection-name*.
config	Displays the complete CBAC or High Availability (HA) inspection configuration.
interfaces	Displays the interface configuration with respect to applied inspection rules and access lists.
sessions [**detail**]	Displays existing sessions that are currently being tracked and inspected by CBAC or HA. The optional **detail** keyword allows additional details about these sessions to be shown.
statistics [**reset**]	Displays CBAC session statistics, such as the number of TCP and HTTP packets that are processed through the inspection, the number of sessions that have been created since the subsystem startup, the current session count, the maximum session count, and the session creation rate. The optional **reset** keyword resets the counters to reflect the latest statistics.
all	Displays all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.
sis [**detail**]	Displays CBAC session information such as window-size information of initiator and responder windows in a session. The optional **detail** keyword allows additional details about these sessions to be shown.

tech-support [**reset**]	Displays additional information regarding drops that are not shown in the **show ip inspect statistics**command. This information is useful for troubleshooting IP inspect issues. The optional **reset** keyword resets the counters to reflect the latest statistics.
vrf *vrf-name*	(Optional) Displays information only for the specified Virtual Routing and Forwarding (VRF) interface.
mib connection-statistics	Displays firewall performance summary statistics that are monitored via firewall MIBs.
global	Displays global connection summary statistics, which are kept for the entire device.
l4-protocol	Displays Layer 4 protocol-based connection summary statistics. Valid values include **all**, **icmp**, **tcp**, **udp**.
l7-protocol [*protocol-type*]	Displays Layer 7 protocol-based connection summary statistics. Refer to the table below for the protocols that can be entered for the *protocol-type* argument.
policy *policy-name*	Displays the name of the firewall policy that is being monitored.
interface	Displays the type of the interface on which the specified firewall policy is applied.
interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(4)T	This command was modified. The output for the **show ip inspect session detail** command was enhanced to support dynamic access control list (ACL) bypass.
12.3(11)T	This command was modified. The **statistics** keyword was added.

Release	Modification
12.3(14)T	This command was modified. The output shows the IMAP and POP3 configuration. The **vrf** *vrf-name*keyword/argument pair was added.
12.4(6)T	This command was modified. • The firewall MIB statistics syntax was added to support firewall performance via SNMP. • High Availability (HA) configuration and session information was added to support Stateful Failover.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.4(11)T	This command was modified. The **tech-support**and **sis** keywords were unhidden and are now supported.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX. Support in a specific 12.2SX release depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to view the CBAC and HA configuration and session information.

ACL Bypass Functionality

ACL bypass allows a packet to avoid redundant ACL checks by allowing the firewall to permit the packet on the basis of existing inspection sessions instead of dynamic ACLs. Because input and output dynamic ACLs have been eliminated from the firewall configuration, the **show ip inspect session detail** command output no longer shows dynamic ACLs. Instead, the output displays the matching inspection session for each packet that is permitted through the firewall.

Firewall MIB Functionality

The Cisco Unified Firewall MIB monitors the following firewall performance statistics:

- Connection statistics, which are a record of the firewall traffic streams that have attempted to flow through the firewall system. Connection statistics can be displayed on a global basis, a protocol-specific basis, or a firewall policy basis.
- URL filtering statistics, which include the status of distinct URL filtering servers that are configured on the firewall and the impact of the performance of the URL filtering servers on the latency and throughput of the firewall.

The table below shows the types of protocols that can be configured for the *protocol-type* argument with the **l7-protocol** keyword:

Table 20: Protocol Types for the l7-protocol Keyword

Protocol-Type	Description
802-11-iapp	IEEE 802.11 WLANs WG IAPP

Protocol-Type	Description
ace-svr	ACE Server/Propagation
all	All protocols
aol	America Online Instant Messenger
appleqtc	Apple QuickTime
bgp	Border Gateway Protocol
biff	Bliff Mail Notification
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
cddbp	CD Database Protocol
cifs	CIFS
cisco-fna	Cisco FNATIVE
cisco-net-mgmt	Cisco Network Management
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs
cisco-sys	Cisco SYSMAINT
cisco-tdp	Cisco Tag Distribution Protocol
cisco-tna	Cisco TNATIVE
citrix	Citrix IMA/ADMIN/RTMP
citirixmaclient	Citrix IMA Client
clp	Cisco Line Protocol
creativepartnr	Creative Partner
creativeserver	Creative Server
cuseeme	CUSeeMe Protocol
daytime	Daytime Protocol (RFC 867)
dbase	dBASE Unix

Protocol-Type	Description
dbcontrol_agent	Oracle Database Control Agent
ddns-v3	Dynamic Domain Name Server Version 3
dhcp-failover	Dynamic Host Control Protocol failover
discard	Discard Protocol
dns	Domain Name Server
dnsix	DNSIX Security Attribute Token Map
echo	Echo Protocol
entrust-svc-hdlr	Entrust KM/Admin Service Handler
entrust-svcs	Entrust sps/aaas/aams
exec	Remote Process Execution
fcip-port	Fibre Channel over IP
finger	Finger Protocol
ftp	File Transfer Protocol
ftps	File Transfer Protocol over Transport Layer Security/ Secure Sockets Layer
gdoi	Group Domain of Interpretation
giop	Oracle GIOP/SSL
gopher	Gopher Protocol
gtpv0	GPRS Tunneling Protocol Version 0
gtpv1	GPRS Tunneling Protocol Version 1
h323	H.323 Protocol for audio-visual communication
h323-annexe	H.323 Protocol AnnexE
h323-nxg	H.323 Protocol AnnexG
hp-alarm-mgr	HP Performance Data Alarm Manager
hp-collector	HP Performance Data Collector

Protocol-Type	Description
hp-managed-node	HP Performance Data Managed Node
hsrp	Hot Standby Router Protocol
http	Hyper Text Transfer Protocol
https	Secure Hyper Text Transfer Protocol
ica	ICA from Citrix
icabrowser	ICA browser from Citrix
ident	Ident Protocol
igmpv3lite	Internet Group Management Protocol over User Datagram Protocol for SSM
imap	Internet Message Access Protocol
imap3	Interactive Mail Access Protocol 3
imaps	IMAP over TLS/SSL
ipass	IPASS
ipsec-msft	Microsoft IPsec NAT-T
ipx	IPX
irc	Internet Relay Chat Protocol
ircs	IRC over TLS/SSL
irc-serv	IRC Serv
ircu	IRCU
isakmp	Internet Security Association and Key Management Protocol
iscsi	Internet Small Computer System Interface
iscsi-target	iSCSI Port
kerberos	Kerberos Protocol
kermit	Kermit Protocol

Protocol-Type	Description
l2tp	Layer 2 Tunneling Protocol
ldap	Lightweight Directory Access Protocol
ldap-admin	LDAP admin server port
ldaps	LDAP over TLS/SSL
login	Remote Login
lotusmtap	Lotus Mail Tracking Agent Protocol
lotusnotes	Lotus Note
mgcp	Media Gateway Control Protocol
microsoft-ds	Microsoft DS
ms-cluster-net	Microsoft Cluster Net
ms-dotnetster	Microsoft .NETster Port
ms-sna	Microsoft SNA Server/Base
ms-sql	Microsoft SQL
ms-sql-m	Microsoft SQL Monitor
msexch-routing	Microsoft Exchange Routing
msnmsgr	MSN Instant Messenger
msrpc	Microsoft Remote Procedure Call
mysql	MySQL
n2h2server	N2H2 Filter Service Port
ncp	NetWare Core Protocol
net8-cman	Oracle Net8 Cman/Admin
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service

Protocol-Type	Description
netshow	Microsoft NetShow
netstat	Network Statistics
nfs	Network File System
nntp	Network News Transport Protocol
ntp	Network Time Protocol
oem-agent	Oracle Enterprise Manager Agent
oracle	Oracle
oracle-em-vp	Oracle Enterprise Manager/VP
oraclenames	Oracle Names
orasrv	Oracle SQL *NET Version 1/2
other	Non-listed Protocols
pcanywheredata	pcAnywhere data
pcanywherestat	pcAnywhere stat
pop3	Post Office Protocol Version 3
pop3s	POP3 over TLS/SSL
pptp	Point-to-Point Tunneling Protocol
pwdgen	Password Generator Protocol
qmtp	Quick Mail Transfer Protocol
radius	RADIUS and Accounting
rdb-dbs-disp	Oracle Relational Database
realmedia	Real Network's Realmedia Protocol
realsecure	ISS Real Secure Console Service Port
router	Local Routing Process
rsvd	RSVD

Protocol-Type	Description
rsvp-encap	RSVP Encapsulation-1/2
rsvp_tunnel	RSVP Tunnel
rtc-pm-port	Oracle RTC-PM Port
rtelnet	Remote Telnet Service
rtsp	Real Time Streaming Protocol
r-winsock	Remote Winsock
send	SEND
shell	Remote Command
sip	Session Initiation Protocol
sip-tls	SIP-TLS
skinny	Skinny Client Control Protocol
sms	SMS
smtp	Simple Mail Transfer Protocol
snmp	Simple Network Management Protocol
snmptrap	SNMP Trap
socks	Socks
sql-net	SQL-NET
sqlserv	SQL Services
sqlsrv	SQL Service
ssh	SSH Remote Login Protocol
sshell	SSLshell
ssp	State Sync Protocol
streamworks	StreamWorks Protocol
stun	Cisco STUN

Protocol-Type	Description
sunrpc	SUN Remote Procedure Call
syslog	Syslog Service
syslog-conn	Reliable Syslog Service
tacacs	Terminal Access Controller Access-Control System
tacacs-ds	TACACS Database Service
tarantella	Tarantella
telnet	Telecommunication Network Protocol.
telnets	Telnet over TLS or SSL
tftp	Trivial File Transfer Protocol
time	Time
timed	Time Server
tr-rsrb	Cisco RSBR
ttc	Oracle TTC or SSL
uucp	Unix-to-Unix Copy Program
vdolive	VDOLive Protocol
vqp	VLAN Query Protocol
webster	Webster Network dictionary
who	Who's Service
wins	Windows Internet Name Service
x11	X Window System
xdmcp	XDM Control Protocol
ymsgr	Yahoo Instant Messenger

Examples

The following is sample output for the **show ip inspect name myinspectionrule**command, where the inspection rule "myinspectionrule" is configured. In this example, the output shows the protocols that should be inspected by CBAC and the corresponding idle timeouts for each protocol.

```
Router# show ip inspect name myinspectionrule
Inspection Rule Configuration
 Inspection name myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

The following is sample output from the **show ip inspect config**command. In this example, the output shows CBAC configuration, including global timeouts, thresholds, and inspection rules.

```
Router# show ip inspect config
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

The following is sample output from the **show ip inspect interfaces**command:

```
Router# show ip inspect interfaces
Interface Configuration
 Interface Ethernet0
  Inbound inspection rule is myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
```

The following is sample output from the **show ip inspect sessions**command. In this example, the output shows the source and destination addresses and port numbers (separated by colons), and it indicates that the session is an FTP session.

```
Router# show ip inspect sessions
Established Sessions
 Session 25A3318 (10.0.0.1:20)=>(10.1.0.1:46068) ftp-data SIS_OPEN
 Session 25A6E1C (10.1.0.1:46065)=>(10.0.0.1:21) ftp SIS_OPEN
```

The following is sample output from the **show ip inspect all**command:

```
Router# show ip inspect all
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
Interface Configuration
 Interface Ethernet0
```

```
  Inbound inspection rule is all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
 Established Sessions
 Session 25A6E1C (10.3.0.1:46065)=>(10.4.0.1:21) ftp SIS_OPEN
 Session 25A34A0 (10.4.0.1:20)=>(10.3.0.1:46072) ftp-data SIS_OPEN
```

The following is sample output from the **show ip inspect session detail**command, which shows that an outgoing ACL and an inbound ACL (dynamic ACLs) have been created to allow return traffic:

```
Router# show ip inspect session detail

Established Sessions
 Session 80E87274 (192.168.1.116:32956)=>(192.168.101.115:23) tcp SIS_OPEN
   Created 00:00:08, Last heard 00:00:04
   Bytes sent (initiator:responder) [140:298] acl created 2
   Outgoing access-list 102 applied to interface FastEthernet0/0
   Inbound access-list 101 applied to interface FastEthernet0/1
```

The following is sample output from the **show ip inspect session detail**command, which shows related ACL information (such as session identifiers [SIDs]), but does not show dynamic ACLs, which are no longer created:

```
Router# show ip inspect session detail
Established Sessions
 Session 814063CC (192.168.1.116:32955)=>(192.168.101.115:23) tcp SIS_OPEN
  Created 00:00:10, Last heard 00:00:06
  Bytes sent (initiator:responder) [140:298]
  HA state: HA_STANDBY
  In  SID 192.168.101.115[23:23]=>192.168.1.117[32955:32955] on ACL 101 (15 matches)
  Out SID 192.168.101.115[23:23]=>192.168.1.116[32955:32955] on ACL 102
```

The following is sample output from the **show ip inspect statistics** command:

```
Router# show ip inspect statistics
Packet inspection statistics [process switch:fast switch]
  tcp packets: [616668:0]
  http packets: [178912:0]
Interfaces configured for inspection 1
Session creations since subsystem startup or last reset 42940
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [98:68:50]
Last session created 5d21h
Last statistic reset never
Last session creation rate 0
Last half-open session total 0
```

The following is sample output from the **show ip inspect tech-support** command:

```
Router# show ip inspect tech-support
Packet inspection statistics [process switch:fast switch]
  tcp packets: [21:879]
Interfaces configured for inspection 1 Pre-gen sessions 0
Session creations since subsystem startup or last reset 19
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [1:1:1]
Last session created 02:25:37
Last statistic reset never
Last session creation rate 0
Last half-open session total 0
Packet disposition statistics [process switch:fastswitch]
  tcp packets dropped: [1:3]
  tcp packets skipped: [0:35]
TCP session reset: 0
```

The following is sample output from the **show ip inspect sis detail** command:

```
Router# show ip inspect sis detail
 Half-open Sessions
 Session 459B498 (75.75.75.3:25471)=>(10.10.10.3:5060) tcp SIS_OPENING
 Created 00:00:01, Last heard 00:00:01
 Bytes sent (initiator:responder) [0:0]
 Initiator->Responder Window size 8000 Scale factor 0
 Responder->Initiator Window size 0 Scale factor 0
Router#
```

The following is sample output from the **show ip inspect mib**command with global or protocol-specific keywords.

Examples

```
Router# show ip inspect mib connection-statistics global
Connections Attempted 7
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 2
Connections Active 3
Connections Expired 2
Connections Aborted 0
Connections Embryonic 0
Connections 1-min Setup Rate 5
Connections 5-min Setup Rate 7
```

Examples

```
Router# show ip inspect mib connection-statistics l4-protocol tcp
Protocol tcp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
Connections 1-min Setup Count 3
Connections 5-min Setup Count 3
Router# show ip inspect mib connection-statistics l7-protocol http
Protocol http
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 2
Connections Resource Declined 0
Connections Half Open 0
Connections Active 1
Connections Aborted 0
Connections 1-min Setup Rate 1
Connections 5-min Setup Rate 2
```

Examples

```
Router# show ip inspect mib connection-statistics policy ftp interface GigabitEthernet0/0
l4-protocol tcp
! Policy Target Protocol Based Connection Summary Stats
Policy ftp-inspection
Target GigabitEthernet0/0
Protocol tcp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
Router# show ip inspect mib connection-statistics policy ftp interface GigabitEthernet0/0
```

```
l7-protocol ftp
! Policy Target Protocol Based Connection Summary Stats
Policy ftp-inspection
Target GigabitEthernet0/0
Protocol ftp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
```

show ip inspect ha

To display stateful failover high availability (HA) session information, use the **show ip inspect ha**command in privileged EXEC mode.

show ip inspect ha [**sessions [detail]** [**vrf** *vrf-name*]| **statistics**]

Syntax Description

sessions	(Optional) Displays information about the sessions.
detail	(Optional) Displays additional information on pinholes created for the return traffic, number of bytes that have passed through this session, and session time information.
vrf *vrf-name*	(Optional) Displays information for the specified virtual routing and forwarding (VRF) instance.
statistics	(Optional) Displays HA sessions statistics for both the active and standby devices.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following is sample output from the **show ip inspect ha sessions**command.

```
Router# show ip inspect ha sessions

Sess_ID  (src_addr:port)=>(dst_addr:port)  proto  sess_state ha_state  Established Session
2CA8958 (10.0.0.5:37690)=>(10.0.0.4:00023) tcp    SIS_OPEN   HA_ACTIVE
```

The table below describes the significant fields shown in the display.

Table 21: show ip inspect ha sessions Field Descriptions

Field	Description
Sess_ID	Displays the session ID.
src_addr:port	Displays source address and port.
dst_addr:port	Displays the destination address and port.

Field	Description
proto	Displays the name of the protocol.
sess_state	Displays the session state.
ha_state	Displays the HA state.
Established Session	Displays the name of the established session.

The following sample output from the **show ip inspect ha sessions detail** command displays additional information for each session.

```
Router# show ip inspect ha sessions detail
Sess_ID  (src_addr:port)=>(dst_addr:port)  proto  sess_state ha_state  Established Session
2CA8958 (10.0.0.5:37690)=>(10.0.0.4:00023) tcp    SIS_OPEN   HA_ACTIVE
 Created 00:01:52, Last heard 00:01:39
 Bytes sent (initiator:responder) [50:91]
 In  SID   10.11.0.4[23:23]=>10.0.0.5[37690:37690] on ACL test  (25 matches)
```

The table below describes the significant fields shown in the display.

Table 22: show ip inspect ha sessions detail Field Descriptions

Field	Description
Created	Displays the date the session was created.
Last heard	Displays the date the packets were received last on the session.
Bytes sent (initiator:responder)	Displays the ratio of bytes sent from the initiator to the responder.
In SID	Session identifier.
on ACL test	Session identifier entry open on an Access Control List (ACL) named test.

The following sample output from the **show ip inspect ha statistics** command displays the following information for the session on the active and standby routers.

On the active router:

```
Router # show ip inspect ha statistics

************************************************
FW HA ACTIVE STATS
************************************************
FW HA active num add session sent             1
FW HA active num delete session sent             0
FW HA active num update session requests             0
FW HA active num update session sent             17
FW HA active bulk sync session             0
FW HA active num error             0
```

```
FW HA active RF error              0
FW HA active CF error              0
FW HA active manager error             0
************************************************
```

On the standby router:

```
Router # show ip inspect ha statistics

************************************************
FW HA STANDBY STATS
************************************************
FW HA standby num add session received             1
FW HA standby num delete session received             0
FW HA standby num update session received            17
FW HA standby num bulk sync request sent             0
FW HA standby num error             0
FW HA standby config error             0
************************************************
```

The table below describes the significant fields shown in the display.

Table 23: show ip inspect ha Field Descriptions

Field	Description
num add session sent	Displays the number of add session messages sent.
num delete session sent	Displays the number of delete session messages sent.
num update session requests	Displays the number of update session message requests.
num update session sent	Displays the number of update session messages sent.
bulk sync session	Displays the number of bulk synchronization requests received.
num error	Displays the number of errors.
RF error	Displays the number of Redundancy Framework (RF) errors.
CF error	Displays the number of Checkpointing Facility (CF) errors.
manager error	Displays the number of manager errors.
bulk sync request sent	Displays the number of bulk synchronization requests sent.
config error	Displays the number of configuration errors.

Related Commands

Command	Description
show ip inspect	Displays CBAC configuration and session information.

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

show ip interface [*type number*] **[brief]**

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Default

The full usability status is displayed for all interfaces configured for IP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The command output was modified to show the status of the **ip wccp redirect out** and **ip wccp redirect exclude add in** commands.
12.2(14)S	The command output was modified to display the status of NetFlow on a subinterface.
12.2(15)T	The command output was modified to display the status of NetFlow on a subinterface.
12.3(6)	The command output was modified to identify the downstream VPN routing and forwarding (VRF) instance in the output.
12.3(14)YM2	The command output was modified to show the usability status of interfaces configured for Multiprocessor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS 12.2(17d)SXB on the Supervisor Engine 2, and the command output was changed to include NDE for hardware flow status.

Release	Modification
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The command output was modified to display information about the Unicast Reverse Path Forwarding (RPF) notification feature.
12.4(20)T	The command output was modified to display information about the Unicast RPF notification feature.
12.2(33)SXI2	This command was modified. The command output was modified to display information about the Unicast RPF notification feature.
Cisco IOS XE Release 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco 4400 Series ISRs.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable (which means that it can send and receive packets). If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry lets the software use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked "up." If the interface hardware is usable, the interface is marked "up."

If you specify an optional interface type, information for that specific interface is displayed. If you specify no optional arguments, information on all the interfaces is displayed.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

You can use the **show ip interface brief** command to display a summary of the router interfaces. This command displays the IP address, the interface status, and other information.

The **show ip interface brief** command does not display any information related to Unicast RPF.

Examples

The following example shows configuration information for interface Gigabit Ethernet 0/3. In this example, the IP flow egress feature is configured on the output side (where packets go out of the interface), and the policy route map named PBRNAME is configured on the input side (where packets come into the interface).

```
Router# show running-config interface gigabitethernet 0/3
interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress
 ip policy route-map PBRNAME
 duplex auto
 speed auto
```

```
 media-type gbic
 negotiation auto
end
```

The following example shows interface information on Gigabit Ethernet interface 0/3. In this example, MPF is enabled, and both Policy Based Routing (PBR) and NetFlow features are not supported by MPF and are ignored.

```
Router# show ip interface gigabitethernet 0/3
GigabitEthernet0/3 is up, line protocol is up
  Internet address is 10.1.1.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN Flow CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
  IP Multi-Processor Forwarding is enabled
     IP Input features, "PBR",
         are not supported by MPF and are IGNORED
     IP Output features, "NetFlow",
         are not supported by MPF and are IGNORED
```

The following example identifies a downstream VRF instance. In the example, "Downstream VPN Routing/Forwarding "D"" identifies the downstream VRF instance.

```
Router# show ip interface virtual-access 3
Virtual-Access3 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
  Broadcast address is 255.255.255.255
  Peer address is 10.8.1.1
  MTU is 1492 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
```

```
  IP Feature Fast switching turbo vector
  IP VPN CEF switching turbo vector
  VPN Routing/Forwarding "U"
  Downstream VPN Routing/Forwarding "D"
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following example shows the information displayed when Unicast RPF drop-rate notification is configured:

```
Router# show ip interface ethernet 2/3
Ethernet2/3 is up, line protocol is up
  Internet address is 10.0.0.4/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Examples

```
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
Router#
```

The following example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1
Vlan1 is up, line protocol is up
```

```
  Internet address is 10.0.0.4/24
  Broadcast address is 255.255.255.255
Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  Sampled Netflow is disabled
  IP multicast multilayer switching is disabled
  Netflow Data Export (hardware) is enabled
```

The table below describes the significant fields shown in the display.

Table 24: show ip interface Field Descriptions

Field	Description
Virtual-Access3 is up	Shows whether the interface hardware is usable (up). For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Broadcast address.
Peer address is	Peer address.
MTU is	MTU value set on the interface, in bytes.
Helper address	Helper address, if one is set.
Directed broadcast forwarding	Shows whether directed broadcast forwarding is enabled.
Outgoing access list	Shows whether the interface has an outgoing access list set.

Field	Description
Inbound access list	Shows whether the interface has an incoming access list set.
Proxy ARP	Shows whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Shows whether split horizon is enabled.
ICMP redirects	Shows whether redirect messages will be sent on this interface.
ICMP unreachables	Shows whether unreachable messages will be sent on this interface.
ICMP mask replies	Shows whether mask replies will be sent on this interface.
IP fast switching	Shows whether fast switching is enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Shows whether Flow switching is enabled for this interface.
IP CEF switching	Shows whether Cisco Express Forwarding switching is enabled for the interface.
Downstream VPN Routing/Forwarding "D"	Shows the VRF instance where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Shows whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast	Shows whether NetFlow is enabled on an interface. Displays "Flow init" to specify that NetFlow is enabled on the interface. Displays "Ingress Flow" to specify that NetFlow is enabled on a subinterface using the **ip flow ingress**command. Shows "Flow" to specify that NetFlow is enabled on a main interface using the **ip route-cache flow** command.
Router Discovery	Shows whether the discovery process is enabled for this interface. It is generally disabled on serial interfaces.

Field	Description
IP output packet accounting	Shows whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Shows whether compression is enabled.
WCCP Redirect outbound is disabled	Shows the status of whether packets received on an interface are redirected to a cache engine. Displays "enabled" or "disabled."
WCCP Redirect exclude is disabled	Shows the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays "enabled" or "disabled."
Netflow Data Export (hardware) is enabled	NetFlow Data Expert (NDE) hardware flow status on the interface.

The table below describes the significant fields shown in the display.

Examples

In the following example, command **show ip interface brief** shows a summary of the interfaces and their status on the device.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/2   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down                  down
Serial1/0/0            unassigned      YES unset  down                  down
GigabitEthernet0       unassigned      YES NVRAM  up                    up
```

Examples

The following example shows how to display a summary of the usability status information for each interface:

```
Router# show ip interface brief
Interface     IP-Address     OK?  Method  Status                  Protocol
Ethernet0     10.108.00.5    YES  NVRAM   up                      up
Ethernet1     unassigned     YES  unset   administratively down   down
Loopback0     10.108.200.5   YES  NVRAM   up                      up
Serial0       10.108.100.5   YES  NVRAM   up                      up
Serial1       10.108.40.5    YES  NVRAM   up                      up
Serial2       10.108.100.5   YES  manual  up                      up
Serial3       unassigned     YES  unset   administratively down   down
```

Table 25: show ip interface brief Field Descriptions

Field	Description
Interface	Type of interface.
IP-Address	IP address assigned to the interface.

Field	Description
OK?	"Yes" means that the IP Address is valid. "No" means that the IP Address is not valid.
Method	The Method field has the following possible values: • RARP or SLARP--Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request. • BOOTP--Bootstrap protocol. • TFTP--Configuration file obtained from the TFTP server. • manual--Manually changed by the command-line interface. • NVRAM--Configuration file in NVRAM. • IPCP--**ip address negotiated** command. • DHCP--**ip address dhcp** command. • unset--Unset. • other--Unknown.
Status	Shows the status of the interface. Valid values and their meanings are: • up--Interface is up. • down--Interface is down. • administratively down--Interface is administratively down.
Protocol	Shows the operational status of the routing protocol on this interface.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.

Command	Description
route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show route-map	Displays static and dynamic route maps.

show ip ips

To display Intrusion Prevention System (IPS) information such as configured sessions and signatures, use the **show ip ips**command in privileged EXEC mode.

Note Effective with Cisco IOS Release 15.1(4)M, the Cisco Services for IPS on IOS feature is not available in Cisco IOS software. As a result, the **license** keyword was removed from this command.

show ip ips {**all**| **configuration**| **interfaces**| **license**| **name** *name*| **sessions [detail]** [**vrf** *vrf-name*]| **signatures** [**[count]** [**detail**| **engine** [*engine-name*]| **sigid** [*sigid* [**subid** [*subid*]]]]| **[statistics]**]| **statistics [reset]** [**vrf** *vrf-name*]}

Syntax Description

all	Displays all available IPS information.
configuration	Displays additional configuration information, including default values that may not be displayed using the **show running-config**command.
interfaces	Displays the interface configuration.
license	Displays license and signature package information.
name *name*	Displays information only for the specified IPS rule.
sessions	Displays IPS session-related information.
detail	(Optional) Shows detailed session information.
vrf *vrf-name*	(Optional) Shows detailed session and latest statistics information per user specific VRF.
signatures	Displays signature information, such as which signatures are disabled and marked for deletion.
count	(Optional) Displays the number of signatures enabled, retired, and compiled.
detail	(Optional) Displays detailed signature information.
engine *engine-name*	(Optional) Displays signatures of a selected engine.
sigid *sigid*	(Optional) Displays signature ID for selected signatures.
subid *subid*	(Optional) Displays the sub ID for selected signatures.

statistics	(Optional) Displays the information such as the number of packets audited and the number of alarms sent.
statistics	Displays the information such as the number of packets audited and the number of alarms sent.
reset	(Optional) Resets sample output to reflect the latest statistics.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	This command was modified. The command name was changed from **show ip audit**to **show ip ips**. Also, all **show ip ips** commands were combined into a single command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
12.4(20)T	This command was modified. The **vrf** *keyword and vrf-name argument were added.*
12.4(22)T	This command was modified. The **count**, **detail**, **engine**, **sigid**, **signatures**, and **subid**keywordsandthe *engine-name*, *subid*, and *sigid*arguments were added.
15.0(1)M	This command was modified. The license keyword was added.
15.1(4)M	This command was modified. The **license** keyword was removed.

Usage Guidelines

Use the **show ip ips configuration** command to display additional configuration information, including default values that may not be displayed using the **show running-config** command.

Examples

Examples

The following example displays the output of the **show ip ips configuration** command:

```
Router# show ip ips configuration
Event notification through syslog is enabled
Event notification through Net Director is enabled
```

```
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)

Audit Rule Configuration
 Audit name AUDIT.1
    info actions alarm
```

Examples The following example displays the output of the **show ip ips interfaces** command:

```
Router# show ip ips interfaces
Interface Configuration
 Interface Ethernet0
  Inbound IPS audit rule is AUDIT.1
    info actions alarm
  Outgoing IPS audit rule is not set
 Interface Ethernet1
  Inbound IPS audit rule is AUDIT.1
    info actions alarm
  Outgoing IPS audit rule is AUDIT.1
    info actions alarm
```

Examples The following example displays the output of the **show ip ips statistics** command:

```
Router# show ip ips statistics
Signature audit statistics [process switch:fast switch]
  signature 2000 packets audited: [0:2]
  signature 2001 packets audited: [9:9]
  signature 2004 packets audited: [0:2]
  signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
Session creations since subsystem startup or last reset 11
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:0]
Last session created 19:18:27
Last statistic reset never

HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0
```

Examples The following example displays the output of the **show ip ips statistics vrf vrf-name**command:

```
Router# show ip ips statistics vrf VRF_600
Signature statistics [process switch:fast switch]
  signature 5170:1 packets checked: [0:2]
Interfaces configured for ips 3
Session creations since subsystem startup or last reset 4
Current session counts (estab/half-open/terminating) [1:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:1]
Last session created 00:02:34
Last statistic reset never
TCP reassembly statistics
  received 8 packets out-of-order; dropped 0
  peak memory usage 12 KB; current usage: 0 KB
  peak queue length 6
```

Examples The following example displays the output of the **show ip ips sessions vrf vrf-name**command:

```
Router# show ip ips sessions vrf VRF_600
```

```
Established Sessions
 Session 67D5C744 (10.0.4.2:34000)=>(10.0.6.2:23) tcp SIS_OPEN
```

Examples

The following example displays the output of the **show ip ips license**command:

```
Router# show ip ips license
IPS License Status Valid
Expiration Date: 2009-12-31
Signatures Loaded: 2009-06-25 S375
Signature Package: 2009-06-25 S375
```

The sample output shows the details for a valid IPS license. Note the license expiration date (2009-12-31), the version date of the existing S375 loaded signatures (2009-07-24 S375), and the version date of the last signature package (S375) loaded (2009-07-24 S375). The license is valid as the existing loaded signature version date is the same as the last signature package version date. The last signature package date (2009-07-24) is also before the license expiration date (2009-12-31).

Related Commands

Command	Description
clear ip ips statistics	Resets statistics on packets analyzed and alarms sent.

show ip ips auto-update

To display the automatic signature update configuration, use the **show ip ips auto-update**command in EXEC mode.

show ip ips auto-update

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing Intrusion Prevention System (IPS) configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **show ip ips auto-update** command to verify the auto update configuration.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration. In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# clock set ?
hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on console.
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml

Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
```

```
Password : not configured
Auto Update Intervals
  minutes (0-59) : 0
  hours (0-23) : 0-23
  days of month (1-31) : 1-31
  days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

show ip ips category

To display the Intrusion Prevention Detection (IPS) categories, use the **show ip ips category** command in user EXEC or privileged EXEC mode.

show ip ips category *category-name* [*subcategory-name*] **[config]**

Syntax Description

category-name	The configured IPS categories. The table in the "Usage Guidelines" lists the *category-name* values.
subcategory-name	(Optional) The configured IPS subcategories. The table in the "Usage Guidelines" lists the *subcategory-name* values.
config	Specifies the configuration values.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **show ip ips category** command to display the IPS categories configured in the network.

The table below lists the values for the*category-name* and *subcategory-name* that can be configured for the **show ip ips category** command:

Table 26: Categories and Subcategories for the show ip ips category Command

Category Name	Description
adware/spyware	Displays information about the configured adware and spyware categories. The subcategory-name can be one of the following values: • **all-adware/spyware** --Advertising-supported software or spyware • **config** --Configuration values

Category Name	Description
attack	Displays information about the configured attack categories. The subcategory-name can be one of the following values: • **code_execution** --Code execution attack • **command_execution** --Command execution attack • **config** --Configuration values • **file_access** --File access • **general_attack** --General attack • **ids_evasion** --Intrusion Detection System (IDS) evasion • **informational** --Attack on the information resident in a network • **policy_violation** --Policy violation
ddos	Displays information about the configured Distributed Denial of Service attack categories. The subcategory-name can be one of the following values: • **all-ddos** --All Distributed Denial of Service attacks • **config** --Configuration values
dos	Displays information about the configured Denial of Service attack categories. The subcategory-name can be one of the following values: • **config** --Configuration values • **icmp_floods** --Internet Control Message Protocol flooding of the network • **tcp_floods** --Transmission Control Protocol flooding of the network • **udp_floods** --User Datagram Protocol flooding of the network

Category Name	Description
email	Displays the configured email clients. The subcategory-name can be one of the following values: • **config** --Configuration values • **imap** --Internet Message Access Protocol • **pop** --Post Office Protocol • **smtp** --Simple Mail Transfer Protocol
instant_messaging	Displays the configured instant messaging clients. The subcategory-name can be one of the following values: • **aol** --America Online • **config** --Configuration values • **jabber** --Jabber instant messaging • **msn** --Microsoft Network • **sametime** --IBM Lotus Sametime Connect • **yahoo** --Yahoo messaging service
ios_ips	Displays signature information, such as the signatures that are disabled or marked for deletion. The subcategory-name can be one of the following values: • **advanced** --Advanced category • **basic** --Basic category • **config** --Configuration values • **default** --Default category

Category Name	Description
l2/l3/l4_protocol	Displays the list of configured Layer 2, Layer 3, and Layer 4 protocols. The subcategory-name can be one of the following values: • **arp** --Address Resolution Protocol • **config** --Configuration values • **general_protocol** --General protocol • **ip** --Internet Protocol. The subcategory-name can be one of the following values: • **config**--Configuration values • **general_ip**--General Internet Protocol • **icmp**--Internet Control Message Protocol • **ip_fragment**--IP Fragment • **ip_v6**--Internet Protocol Version 6 • **tcp**--Transmission Control Protocol • **udp**--User Datagram Protocol
network_services	Displays the configured routing protocols. The subcategory-name can be one of the following values: • **bgp** --Border Gateway Protocol • **config** --Configuration values • **dhcp** --Dynamic Host Configuration Protocol • **dns** --Domain Name Server • **finger** --Finger User Information Protocol

Category Name	Description

os	Displays the configured operating system. The subcategory-name can be one of the following values:
	• **config** --Configuration values
	• **general_os** --General operating system
	• **ios** --Internetwork Operating System
	• **mac_os** --Mac operating system
	• **netware** --Netware operating system
	• **unix** --UNIX operating systems. The subcategory-name can be one of the following values:
	  • **aix**--Advanced Interactive eXecutive operating system
	  • **config**--Configuration values
	  • **general-unix**--UNIX operating system
	  • **hp-ux**--Hewlett-Packard UNIX operating system
	  • **irix**--IRIX operating system
	  • **linux**--Linux operating system
	  • **solaris**--Solaris operating system
	• **windows** --Windows operating systems. The subcategory-name can be one of the following values:
	  • **config**--Configuration values
	  • **general_windows**--General Windows
	  • **windows_nt/2k/xp**--Windows NT, Windows 2000, or Windows XP operating systems. You can specify the following keywords: **config**, **general_windows_nt/2k/xp**, and **winnt**.

Category Name	Description
other_services	Displays the other protocols configured. The subcategory-name can be one of the following values: • **config** --Configuration values • **ftp** --File Transfer Protocol • **general_service** --General service • **http** --Hypertext Transfer Protocol • **https** --Hypertext Transfer Protocol Secure • **ident** --Ident protocol • **lpr** --Line Printer Daemon protocol • **msrpc** --Microsoft Remote Procedural Call • **netbios/smb** --Network Basic Input/Output System or Server Message Block • **nntp** --Network News Transfer Protocol • **ntp** --Network Time Protocol • **r-services** --R services • **rpc** --Remote Procedural Call • **snmp** --Simple Network Management Protocol • **socks** --SOCKS • **sql** --Structured Query Language • **ssh** --Secure Shell Remote Protocol • **telnet** --Telnet Remote Protocol • **tftp** --Trivial File Transport Protocol
p2p	Displays the configured peer-to-peer networks for file sharing. The subcategory-name can be one of the following values: • **bittorrent** --BitTorrent • **config** --Configuration values • **edonkey** --eDonkey • **kazaa** --Kazaa

Category Name	Description
reconnaissance	Displays the configured network reconnaissance categories. The subcategory-name can be one of the following values: • **config** --Configuration values • **icmp_host_sweeps** --Internet Control Message Protocol Host Sweeps • **tcp/udp_combo_sweeps** --Transmission Control Protocol or User Datagram Protocol Combo Sweeps • **tcp_ports_sweeps** --Transmission Control Protocol Port Sweeps • **udp_port_sweeps** --User Datagram Protocol Port Sweeps
viruses/worms/trojans	Displays the viruses, worms, and trojans against which the network is configured. The subcategory-name can be one of the following values: • **all-viruses/worms/trojans** --All viruses, worms, and trojans that attack a network • **config** --Configuration values
web_server	Displays the configured Web servers. The subcategory-name can be one of the following values: • **apache** --Apache Web server • **config** --Configuration values • **internet_information_server_(iis)** --IIS Web server

Examples

The following examples display the output from variations of the **show ip ips category** command. The field names are self-explanatory.

```
Router# show ip ips category attack

Signatures in command_execution:
Signatures in general_attack:
Signatures in informational:
Signatures in file_access:
Signatures in code_execution:
Signatures in policy_violation:
Signatures in ids_evasion:
Router# show ip ips category instant_messaging

Signatures in yahoo:
```

```
Signatures in aol:
Signatures in msn:
Signatures in sametime:
Signatures in jabber:
```

Related Commands

Command	Description
ip ips	Applies an IPS rule to an interface.

show ip ips event-action-rules

To display event action rules information, use the **show ip ips event-action-rules** command in privileged EXEC mode.

show ip ips event-action-rules {**filters**| **overrides**| **target-value-rating**}

Syntax Description

filters	Displays the signature event action filters.
overrides	Displays the signature event action overrides.
target-value-rating	Displays the target value rating.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4 (11)T	This command was introduced.

Usage Guidelines

Event action rules are a group of settings you configure for the event action processing component of the sensor. These rules dictate the actions the sensor performs when an event occurs. Use the **show ip ips event-action-rules** command to display event action rules information, including default values that may not be displayed using the **show running-config** command.

Examples

The following example shows the global filter status for the event-action-rules. The output is self-explanatory.

```
Router# show ip ips event-action-rules filters

Filters
Global Filters Status: Enabled
```

The following example shows the global overrides status for the event-action-rules. The output is self-explanatory.

```
Router# show ip ips event-action-rules overrides

Overrides
Global Overrides Status: Enabled
Action to Add                    Enabled  Risk Rating
```

The following example shows the target-value-rating configuration status for the event-action-rules.The output is self-explanatory.

```
Router# show ip ips event-action-rules target-value-rating
No Target Value Ratings are configured
```

Related Commands

Command	Description
category	Displays category information.
configuration	Displays the IPS configuration information.
interfaces	Displays the IPS interfaces information.
ip ips all	Displays all IPS information.
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
name	Displays IPS name.
sessions	Displays IPS sessions.
signature-category	Displays signature category.
signatures	Displays IPS signatures.
statistics	Resets statistics on packets analyzed and alarms sent.

show ip ips signature-category

To display Cisco IOS Intrusion Prevention System (IPS) signature parameters by signature category, use the **show ip ips signature-category** command in privileged EXEC mode.

show ip ips signature-category [config]

Syntax Description

config	(Optional) Specifies configuration parameters for the signature categories.

Command Default

All the available signatures for the categories are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **show ip ips signature-category**command to verify the IPS signature parameters configured on the basis of a signature category.

Examples

The following is sample output from the **show ip ips signature-category** command:

```
Router# show ip ips signature-category
Signatures in basic:
Signatures in advanced:
Signatures in general_unix:
Signatures in general_linux:
Signatures in redhat:
Signatures in gentoo:
Signatures in mandrake:
Signatures in suse:
Signatures in solaris:
Signatures in hp-ux:
Signatures in aix:
Signatures in irix:
Signatures in general_windows:
Signatures in general_windows_nt/2k/xp:
Signatures in winnt:
Signatures in ios:
Signatures in general_os:
Signatures in netware:
Signatures in mac_os:
Signatures in command_execution:
Signatures in general_attack:
Signatures in informational:
Signatures in file_access:
```

The following example shows the **show ip ips signature-category**command output with the configured signature parameters:

```
Router# show ip ips signature-category config
    Category all:
        Retire: True
    Category IOSIPS 256mb:
        Retire: False
```

Related Commands

Command	Description
ip ips signature-category	Tunes IPS signature parameters per category.
show ip ips	Displays IPS configuration information.

show ip nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ip nhrp nhs**command in user EXEC or privileged EXEC mode.

show ip nhrp nhs [*interface*] **[detail]**

Syntax Description

interface	(Optional) Displays NHS information currently configured on the interface. See the table below for types, number ranges, and descriptions.
detail	(Optional) Displays detailed NHS information.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface*argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 27: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix

Valid Types	Number Ranges	Interface Descriptions
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ip nhrp nhs detail** command:

```
Router# show ip nhrp nhs detail
Legend:
  E=Expecting replies
  R=Responding
Tunnel1:
  5.1.1.1           E  req-sent 128  req-failed 1  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 5.1.1.1
```

The table below describes the significant field shown in the display.

Table 28: show ip nhrp nhs Field Descriptions

Field	Description
Tunnel1	Interface through which the target network is reached.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	Displays NHRP traffic statistics.

show ip port-map

To display the port-to-application mapping (PAM) information, use the show ip port-map command in privileged EXEC mode.

show ip port-map [*appl-name*| **port** *port-num* **[detail]**]

Syntax Description

appl-name	(Optional) Specifies the name of the application to which to apply the port mapping.
port *port-num*	(Optional) Specifies the alternative port number that maps to the application.
detail	(Optional) Shows the port or application details.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(14)T	The **detail** keyword was added and command output was modified to display user-defined applications.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display the port mapping information at the firewall, including the system-defined and user-defined information. Include the application name to display the list of entries by application. Include the port number to display the entries by port.

Examples

The following is sample output from the **show ip port-map** command, including system- and user-defined mapping information. Notice that multiple port numbers display in a series such as 554, 8554, or 1512...1525, or a range such as 55000 to 62000. When there are multiple ports, they all display if they can fit into the fixed-field width. If they cannot fit into the fixed-field width, they display with an ellipse, such as 1512...1525 shown below.

```
Router# show ip port-map
Default mapping:  snmp       udp port 161                    system defined
```

```
Host specific:    snmp       udp port 577         in list 55 user defined
Host specific:    snmp       udp port 55000-62000 in list 57 user defined
Default mapping:  echo       tcp port 7                      system defined
Default mapping:  echo       udp port 7                      system defined
Default mapping:  telnet     tcp port 23                     system defined
Default mapping:  wins       tcp port 1512...1525            system defined
Default mapping:  n2h2server tcp port 9285                   system defined
Default mapping:  n2h2server udp port 9285                   system defined
Default mapping:  nntp       tcp port 119                    system defined
Default mapping:  pptp       tcp port 1725                   system defined
Default mapping:  rtsp       tcp port 554,8554               system defined
Default mapping:  bootpc     udp port 68                     system defined
Default mapping:  gdoi       udp port 848                    system defined
Default mapping:  tacacs     udp port 49                     system defined
Default mapping:  gopher     tcp port 70                     system defined
Default mapping:  icabrowser udp port 1604                   system defined
```

The following sample output from the **show ip port-map snmp** command displays information about the SNMP application:

```
Router# show ip port-map snmp
Default mapping:  snmp    udp port 161                     system defined
Host specific:    snmp    udp port 577          in list 55  user defined
Host specific:    snmp    udp port 55000-62000  in list 57  user defined
```

The following sample output from the **show ip port-map snmp detail** command displays detailed information about the SNMP application:

```
Router# show ip port-map snmp detail
 IP port-map entry for application 'snmp':
     udp 161                  Simple Network Management Protoco system defined
     udp 577            list 55 User's SNMP Port                 user defined
     udp 55000-62000    list 57 User's Another SNMP Port         user defined
```

The following sample output from the **show ip port-map port 577** command displays information about port 577:

```
Router# show ip port-map port 577
Host specific:   snmp  udp port 577    in list 55   user defined
```

The following sample output from the **show ip port-map port 55800**command displays information about port 55800:

```
Router# show ip port-map port 55800
Host specific:   snmp   udp port 55800  in list 57   user defined
```

The following sample output from the **show ip-port-map port 577 detail** command displays detailed information about port 577:

```
Router# show ip port-map port 577 detail

 IP Port-map entry for port 577:
 snmp                udp list 55                           user defined
```

Related Commands

Command	Description
ip port-map	Establishes PAM entries.

show ip sdee

To display Security Device Event Exchange (SDEE) notification information, use the **show ip sdee**command in privileged EXEC mode.

show ip sdee [alerts] [all] [errors] [events] [configuration] [status] [subscriptions]

Syntax Description

alerts	Displays the Intrusion Detection System (IDS) alert buffer.
all	Displays all information available for IDS SDEE notifications.
errors	Displays IDS SDEE error messages.
events	Displays IDS SDEE events.
configuration	Displays SDEE configuration parameters.
status	Displays the status events that are currently in the buffer.
subscriptions	Displays IDS SDEE subscription information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from the **show ip sdee alerts** command. In this example, the alerts are numbered from 1 to 100 (because 100 events are currently in the event buffer). Following the alert number are 3 digits, which indicate whether the alert has been reported for the 3 possible subscriptions. In this example, these alerts have been reported for subscription number 1. The event ID is composed of the alert time and an increasing count, separated by a colon.

```
Router# show ip sdee alerts
Event storage:1000 events using 656000 bytes of memory
                                SDEE Alerts
SigID       SrcIP     DstIP       SrcPort  DstPort  Sev     Event ID        SigName
1:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211478597901  ICMP Echo Req
2:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211478887902  ICMP Echo Req
3:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479247903  ICMP Echo Req
4:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479457904  ICMP Echo Req
```

```
5:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479487905  ICMP Echo Req
6:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211480077906  ICMP Echo Req
7:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211480407907  ICMP Echo Req
.....................................................
.....................................................
96:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898596  ICMP Echo Req
97:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898597  ICMP Echo Req
98:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898598  ICMP Echo Req
99:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750908599  ICMP Echo Req
100:000 2004 10.0.0.2 10.0.0.1    8        0        2       10211750918600  ICMP Echo Req
```

The following is sample output is from the **show ip sdee subscriptions**command. In this example, SDEE is enabled, the maximum event buffer size has been set to 100, and the maximum number of subscriptions that can be open at the same time is 1.

```
Router# show ip sdee subscriptions

SDEE is enabled
Alert buffer size:100 alerts 65600 bytes
Maximum subscriptions:1
SDEE open subscriptions: 1
Subscription ID IDS1720:0:
Client address 10.0.0.2 port 1500
        Subscription opened at 13:21:30 MDT July 18 2003
        Total GET requests:0
        Max number of events:50
        Timeout:30
        Event Start Time:0
        Report alerts:true
        Alert severity level is INFORMATIONAL
        Report errors:false
        Report status:false
```

The table below describes the significant fields shown in the display.

Table 29: show ip sdee subscriptions Field Descriptions

Field	Description
Alert buffer size:100 alerts 65600 bytes	Maximum number of events that can be stored in the buffer. The maximum number of events to be stored refers to all types of events (alert, status, and error). (This value can be changed via the **ip sdee events** command.)
Maximum subscriptions:1	Maximum number of subscriptions that can be open at the same time. (This value can be changed via the **ip sdee subscriptions** command.)

The following is sample output from the **show ip sdee status**command. In this example, the buffer is set to store a maximum of 1000 events.

```
Router# show ip sdee status
Event storage:1000 events using 656000 bytes of memory
                  SDEE Status Messages
Time                          Message              Description
1:000 22:10:58 UTC Apr 18 2003  applicationStarted   STRING.UDP,0 ms
2:000 22:10:58 UTC Apr 18 2003  applicationStarted   STRING.TCP,0 ms
3:000 22:10:58 UTC Apr 18 2003  applicationStarted   OTHER,0 ms
4:000 22:10:58 UTC Apr 18 2003  applicationStarted   SERVICE.FTP,276 ms
5:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.SMTP,8884 ms
6:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.RPC,72 ms
7:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.DNS,132 ms
```

```
8:000 22:11:15 UTC Apr 18 2003  applicationStarted   SERVICE.HTTP,7632 ms
9:000 22:11:15 UTC Apr 18 2003  applicationStarted   ATOMIC.TCP,24 ms
10:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.UDP,12 ms
11:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.ICMP,12 ms
12:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.IPOPTIONS,8 ms
13:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.L3.IP,8 ms
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.
id sdee events	Sets the maximum number of SDEE events that can be stored in the event buffer.
ip sdee subscriptions	Sets the maximum number of SDEE subscriptions that can be open simultaneously.

show ip ips sig-clidelta

To display the signature parameter tunings configured using the CLI that are stored in the iosips-sig-clidelta.xmz signature file, use the **show ip ips sig-clidelta**command in privileged EXEC mode.

show ip ips sig-clidelta

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show ip ips sig-clidelta**command displays the tunings configured from the CLI that are stored in the iosips-sig-clidelta.xmz signature file.

Examples

The following is sample output from the **show ip ips sig-clidelta**command. The field descriptions are self-explanatory.

```
Router# show ip ips sig-clidelta
En  - possible values are Y, Y*, N, or N*
      Y:  signature is enabled
      N:  enabled=false in the signature definition file
      *:  retired=true in the signature definition file
Cmp - possible values are Y, Ni, Nr, Nf, or No
      Y:  signature is compiled
      Ni: signature not compiled due to invalid or missing parameters
      Nr: signature not compiled because it is retired
      Nf: signature compile failed
      No: signature is obsoleted
      Nd: signature is disallowed
Action=(A)lert, (D)eny, (R)eset, Deny-(H)ost, Deny-(F)low
Trait=alert-traits             EC=event-count          AI=alert-interval
GST=global-summary-threshold   SI=summary-interval     SM=summary-mode
SW=swap-attacker-victim        SFR=sig-fidelity-rating Rel=release
 SigID:SubID En  Cmp   Action Sev   Trait   EC   AI   GST   SI  SM SW SFR Rel
 ----------- --  ----  ------ ---   -----  ---- ---- -----  --- -- -- --- ---
  5733:0     N   Y     A     HIGH     0     1    0      0    0  FA  N 85  S266
```

Related Commands

Command	Description
ip ips enable-clidelta	Enables the signature tuning settings in the clidelta.xmz file on the router to take precedence over the signature settings in the iosips-sig-delta.xmz file.

show ip source-track

To display traffic flow statistics for tracked IP host addresses, use the **show ip source-track**command in privileged EXEC mode.

show ip source-track [*ip-address*] [**summary**| **cache**]

Syntax Description

ip-address	(Optional) Displays the IP address of the tracked host for which traffic flow information is displayed.
summary	(Optional) Displays a summary of traffic flow information that is collected for a specified host address (via the *ip-address* argument) or for all configured hosts.
cache	(Optional) Displays detailed packet and flow information that is collected on line cards and port adapters for all tracked IP addresses or for specified IP address (not displayed in the a distributed platform such as the gigabit route processor (GRP) or route switch processor (RSP)).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example, which is sample output from the show ip source-track summary command, shows how to verify that IP source tracking is enabled for one or more hosts:

```
Router# show ip source-track summary
Address          Bytes    Pkts    Bytes/s   Pkts/s
10.0.0.1          119G   1194M    443535      4432
192.168.1.1       119G   1194M    443535      4432
192.168.42.42     119G   1194M    443535      4432
```

The following example, which is sample output from the show ip source-track summary command, shows how to verify that no traffic has yet to be received for the destination hosts that are being tracked:

```
Router# show ip source-track summary
Address        Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1           0      0         0        0
192.168.1.1        0      0         0        0
192.168.42.42      0      0         0        0
```

The following example, which is sample output from the show ip source-track command, shows that IP source tracking is processing packets to the hosts and exporting statistics from the line card or port adapter to the route processor:

```
Router# show ip source-track
Address         SrcIF    Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1        PO0/0    119G   1194M    513009     5127
192.168.1.1     PO0/0    119G   1194M    513009     5127
192.168.42.42   PO0/0    119G   1194M    513009     5127
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
ip source-track address-limit	Configures the maximum number of destination hosts that can be simultaneously tracked at any given moment.
ip source-track syslog-interval	Sets the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device.

show ip source-track export flows

To display the last ten packet flows that were exported from the line card to the route processor, use the **show ip source-track export flows**command in privileged EXEC mode.

show ip source-track export flows

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show ip source-track export flows** command can be issued only on distributed platforms such as the GRP and the RSP.

Examples

The following example displays the packet flow information that is exported from line cards and port adapters to the gigabit route processor (GRP) and the route switch processor (RSP):

```
Router# show ip source-track export flows
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
PO0/0         10.1.1.0        Null          10.1.1.1        06 0000 0000    88K
PO0/0         10.1.1.0        Null          10.1.1.3        06 0000 0000    88K
PO0/0         10.1.1.0        Null          10.1.1.2        06 0000 0000    88K
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.

Command	Description
ip source-track export-interval	Sets the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the RP.

show ip ssh

To display the version and configuration data for Secure Shell (SSH), use the **show ip ssh** command in privileged EXEC mode.

show ip ssh

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.
12.1(5)T	This command was modified to display the SSH status--enabled or disabled.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **show ip ssh** command to view the status of configured options such as retries and timeouts. This command allows you to see if SSH is enabled or disabled.

Examples

The following is sample output from the **show ip ssh** command when SSH has been enabled:

```
Router# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
The following is sample output from the show ip ssh
 command when SSH has been disabled:
Router# show ip ssh
%SSH has not been enabled
```

Related Commands

Command	Description
show ssh	Displays the status of SSH server connections.

show ip traffic-export

To display information related to router IP traffic export (RITE), use the **show ip traffic-export**command in privileged EXEC mode.

show ip traffic-export [**interface** *interface-name*| **profile** *profile-name*]

Syntax Description

interface *interface-name*	(Optional) Only data associated with the monitored ingress interface is shown.
profile *profile-name*	(Optional) Only flow statistics, such as exported packets and number of bytes, are shown.

Command Default

If this command is enabled, all data (both interface- and profile-related data) is shown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following sample output from the **show ip traffic-export**command is for the profile "one." This example is for a single configured interface. If multiple interfaces are configured, the information shown below is displayed for each interface.

```
Router# show ip traffic-export
Router IP Traffic Export Parameters
Monitored Interface FastEthernet0/0
Export Interface FastEthernet0/1
Destination MAC address 0030.7131.abfc
bi-directional traffic export is off
```

Input IP Traffic Export Information Packets/Bytes Exported 0/0

Packets Dropped 0

Sampling Rate one-in-every 1 packets

```
No Access List configured
Profile one is Active
```

The table below describes the significant fields shown in the display.

Table 30: show ip traffic-export Field Descriptions

Field	Description
Monitored Interface	Interface in which the profile was applied. (This interface is specified via the **ip traffic-export apply profile** command.)
Export Interface	Interface in which the profile exports all captured IP traffic. (This interface is specified via the **ip traffic-export profile** command.)
Destination MAC address	Ethernet address of the destination host, which is specified via the **mac-address** command.
bi-directional traffic export is	Incoming and outgoing IP traffic is exported on the monitored interface (via the **bidirectional** command). By default, only incoming traffic is exported.
Input IP Traffic Export Information Packets Dropped Sampling Rate No Access List Configured Profile one is Active	Incoming IP traffic information. The sampling rate and ACL can be defined via the **incoming** command. If the profile is incomplete, the profile will be listed as inactive.

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported across a monitored interface.
ip traffic-export apply profile	Applies an IP traffic export profile to a specific interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
incoming	Configures filtering for incoming export traffic.
outgoing	Configures filtering for outgoing export traffic.

show ip trigger-authentication

To display the list of remote hosts for which automated double authentication has been attempted, use the **show ip trigger-authentication** command in privileged EXEC mode.

show ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Whenever a remote user needs to be user-authenticated in the second stage of automated double authentication, the local device sends a User Datagram Protocol (UDP) packet to the remote user's host. When the UDP packet is sent, the user's host IP address is added to a table. If additional UDP packets are sent to the same remote host, a new table entry is not created; instead, the existing entry is updated with a new time stamp. This remote host table contains a cumulative list of host entries; entries are deleted after a timeout period or after you manually clear the table using the **clear ip trigger-authentication** command. You can change the timeout period with the **ip trigger-authentication**(global) command.

Use this command to view the list of remote hosts for which automated double authentication has been attempted.

Examples

The following example shows output from the **show ip trigger-authentication** command:

```
Router# show ip trigger-authentication
Trigger-authentication Host Table:
Remote Host          Time Stamp
209.165.200.230       2940514234
```

This output shows that automated double authentication was attempted for a remote user; the remote user's host has the IP address 209.165.200.230. The attempt to automatically double authenticate occurred when the local host (myfirewall) sent the remote host (209.165.200.230) a packet to UDP port 7500. (The default port was not changed in this example.)

Related Commands

Command	Description
clear ip trigger-authentication	Clears the list of remote hosts for which automated double authentication has been attempted.

show ip trm subscription status

To display information about the status of the Trend Micro subscription, use the **show ip trm subscription status**command in privileged EXEC mode.

show ip trm subscription status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show ip trm subscription status**command to display the status of the Trend Micro subscription. If the router is registered with the Trend Router Provisioning Server (TRPS), the router displays the subscription status information. If the router is not registered with the TRPS, a message indicating that the router is not registered is displayed.

Examples

The following shows sample output from **show ip trm subscription status**command when the router is registered with the TRPS:

```
Router# show ip trm subscription status

Package Name: Security & Productivity
 ------------------------------------------------
    Status:     Active
 Status Update Time:     08:55:07 MDT Thu Apr 3 2008
    Expiration-Date:     Tue Jul 21 10:12:59 2020

    Last Req Status:     Processed response successfully
 Last Req Sent Time:     08:55:07 MDT Thu Apr 3 2008
```

The table below describes the significant fields shown in the display.

Table 31: show ip trm subscription status Field Descriptions

Field	Description
Status	Displays the status of the Trend Micro subscription.
Status Update Time	Displays the time and date that status of the Trend Micro subscription was last updated.

Field	Description
Expiration Date	Displays the date and time that the Trend Micro subscription expires.
Last Req Status	Displays the status of the most recent request.
Last Req Sent Time	Displays the time and date of the most recent lookup request to the TRPS.

Related Commands

Command	Description
show ip trm config	Displays information about the TRPS.

show ip urlfilter

To display URL filtering information, use the **show ip urlfilter** command in privileged EXEC mode.

show ip urlfilter {**mib statistics** {**global**| **server** {**address** *ip-address* [**port** *port-number*]| **all**}}| **statistics** [**vrf** *vrf-name*]}

Syntax Description

mib	Displays the firewall MIB-specific URL filtering content.
statistics	Displays URL filtering statistics for the specified parameters.
global	Displays global URL filtering statistics.
server	Displays statistics for the specified server.
address *ip-address*	Displays URL filtering information for the server with the specified IP address.
port *port-number*	(Optional) Displays statistics for the specified server using the service port.
all	Displays statistics for all configured servers.
vrf *vrf-name*	(Optional) Displays information about a specified virtual routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.4(6)T	This command was modified. The following keywords and arguments were added: **all**, **address**, **global**, *ip-address*, **mib**, **port**, *port-number*, and **server**.

Usage Guidelines

The firewall interacts with URL filtering to prevent users from accessing specified websites on the basis of configured policies such as destination hostname, destination IP address, keyword, and username. Use the **show ip urlfilter** command to display the URL filtering information such as the number of requests that are sent to the vendor server (Websense or N2H2), the number of responses received from the vendor server, the number of pending requests in the system, the number of failed requests, and the number of blocked URLs.

Examples

The following is sample output from the **show ip urlfilter statistics** command:

```
Device# show ip urlfilter statistics

URL filtering statistics
================
Current requests count:25
Current packet buffer count(in use):40
Current cache entry count:3100
Maxever request count:526
Maxever packet buffer count:120
Maxever cache entry count:5000
Total requests sent to URL Filter Server: 44765
Total responses received from URL Filter Server: 44550
Total requests allowed: 44320
Total requests blocked: 224
```

The table below describes the significant fields shown in the display.

Table 32: show ip urlfilter statistics Field Descriptions

Field	Description
Current requests count	Number of requests sent to the vendor server.
Current packet buffer count (in use)	Number of HTTP responses in the packet buffer of the firewall. This value can be specified by using the **ip urlfilter max-resp-pak** command.
Current cache entry count	Number of destination IP addresses cached into the cache table. This value can be specified by using the **ip urlfilter cache** command.
Maxever request count	Maximum number of requests that are sent to the vendor server since power up. This value can be specified by using the **ip urlfilter max-request** command.
Maxever packet buffer count	Maximum number of HTTP responses stored in the packet buffer of the firewall since power up. This value can be specified by using the **ip urlfilter max-resp-pak** command.
Maxever cache entry count	Maximum number of destination IP addresses that are cached in the cache table since power up. This value can be specified by using the **ip urlfilter cache** command.

The following is sample output from the **show ip urlfilter mib statistics global** command when MIBs are enabled to track URL filtering statistics across the entire device (global). The output fields are self-explanatory.

```
Device# show ip urlfilter mib statistics global

URL Filtering Group Summary Statistics
------------------------------------------------------
URL Filtering Enabled
Requests Processed 260
Requests Processed 1-minute Rate 240
Requests Processed 5-minute Rate 215
Requests Allowed 230
Requests Denied 30
Requests Denied 1-minute Rate 15
Requests Denied 5-minute Rate 0
Requests Cache Allowed 5
Requests Cache Denied 5
Allow Mode Requests Allowed 15
Allow Mode Requests Denied 15
Requests Resource Dropped 0
Requests Resource Dropped 1-minute Rate 0
Requests Resource Dropped 5-minute Rate 0
Server Timeouts 0
Server Retries 0
Late Server Responses 0
Access Responses Resource Dropped 0
```

The following is sample output from the **show ip urlfilter mib statistics server address** command when MIBs are enabled to track URL filtering statistics across the server with the IP address 209.165.201.30. The output fields are self-explanatory.

```
Device# show ip urlfilter mib statistics server address 209.165.201.30

URL Filtering Server Statistics
------------------------------------------------------
URL Server Host Name 209.165.201.30
Server Address 209.165.201.30
Server Port 15868
Server Vendor Websense
Server Status Online
Requests Processed 4
Requests Allowed 1
Requests Denied 3
Server Timeouts 0
Server Retries 9
Responses Received 1
Late Server Responses 12
1 Minute Average Response Time 0
5 Minute Average Response Time 0
```

Related Commands

Command	Description
ip urlfilter cache	Configures cache parameters.
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.
ip urlfilter max-resp-pak	Configures the maximum number of HTTP responses that the firewall can keep in its packet buffer.

show ip urlfilter cache

To display the maximum number of entries that can be cached and the number of entries and destination IP addresses that are cached into the cache table, use the **show ip urlfilter cache** command in privileged EXEC mode.

show ip urlfilter cache [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about a specified virtual routing and forwarding (VRF) interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on the feature set, platform, and platform hardware.

Usage Guidelines

The output from the **show ip urlfilter cache** command displays the number of entries cached by a device.

The IP cache table consists of the most recently requested IP addresses and the respective authorization status for each IP address. Use the **show ip urlfilter cache** command to view the contents of the cache table.

Examples

The following is sample output from the **show ip urlfilter cache** command:

```
Device# show ip urlfilter cache

Maximum number of entries allowed: 5000
Number of entries cached: 5
IP addresses cached ....
 10.64.128.54
 172.28.139.21
 10.76.82.25
 192.168.0.1
 10.0.1.2
```

The following table describes the fields shown in the display.

Table 33: show ip urlfilter cache Field Descriptions

Field	Description
Maximum number of entries allowed	Maximum number of destination IP addresses that can be cached into the cache table. This parameter can be configured using the **ip url filter cache** command. The default is 5000.
Number of entries cached	Number of entries that have already been cached into the cache table.
IP addresses cached	IP addresses that have already been cached into the cache table.

Related Commands

Command	Description
clear ip urlfilter cache	Clears the cache table.
ip urlfilter cache	Configures cache parameters.

show ip urlfilter config

To display the size of the cache, the maximum number of outstanding requests, the allow mode state, and the list of configured vendor servers, use the **show ip urlfilter config**command in EXEC mode.

show ip urlfilter config [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Modes

EXEC

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair was added.

Examples

The following example is sample output from the **show ip urlfilter config** command:

```
Router# show ip urlfilter config
URL filter is ENABLED
Primary Websense server configurations
==========================
Websense server IP address: 10.0.0.3
Websense server port: 15868
Websense retransmit time out: 5 (seconds)
Websense number of retransmit:2
Secondary Websense server configurations:
============================
None.
Other configurations
===============
Allow mode: OFF
System Alert: ON
Log message on the router: OFF
Log message on URL filter server:ON
Maximum number of cache entries :5000
Cache timeout :12 (hours)
Maximum number of packet buffers:200
Maximum outstanding requests:1000
```

Related Commands

Command	Description
ip urlfilter allowmode	Turns on the default mode (allow mode) of the filtering algorithm.
ip urlfilter cache	Configures cache parameters.
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.
ip urlfilter server vendor	Configures a vendor server for URL filtering.

show ip virtual-reassembly

To display the configuration and statistical information of the virtual fragment reassembly (VFR) on a given interface, use the **show ip virtual-reassembly** command in privileged EXEC mode.

show ip virtual-reassembly [**interface** *type*]

Syntax Description

interface *type*	(Optional) VFR information is shown only for the specified interface. If an interface is not specified, VFR information for all configured interfaces is shown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example is sample output from the **show ip virtual-reassembly** command:

```
Router# show ip virtual-reassembly interface ethernet1/1
Ethernet1/1:
Virtual Fragment Reassembly (VFR) is ENABLED...
Concurrent reassemblies (max-reassemblies):64
Fragments per reassembly (max-fragments):16
Reassembly timeout (timeout):3 seconds
Drop fragments:OFF
Current reassembly count:12
Current fragment count:48
Total reassembly count:6950
Total reassembly failures:9
```

The table below describes the significant fields shown in the display.

Table 34: show ip virtual-reassembly Field Descriptions

Field	Description
Concurrent reassemblies (max-reassemblies):64	Maximum number of IP datagrams that can be reassembled at any given time. Value can be specified via the **max-reassemblies** *number*option from the **ip virtual-reassembly** command.

Field	Description
Fragments per reassembly (max-fragments):16	Maximum number of fragments that are allowed per IP datagram (fragment set). Value can be specified via the **max-fragments** *number* option from the **ip virtual-reassembly** command.
Reassembly timeout (timeout):3 seconds	Timeout value for an IP datagram that is being reassembled. Value can be specified via the **timeout** *seconds* option from the **ip virtual-reassembly** command.
Drop fragments:OFF	Specifies whether the VFR should drop all fragments that arrive on the configured interface. Function can be turned on or off via the **drop-fragments** keyword from the **ip virtual-reassembly** command.
Current reassembly count	Number of IP datagrams that are currently being reassembled
Current fragment count	Number of fragments that have been buffered by VFR for reassembly
Total reassembly count	Total number of datagrams that have been reassembled since the last system reboot.
Total reassembly failures	Total number of reassembly failures since the last system reboot.

Related Commands

Command	Description
ip virtual-reassembly	Enables VFR on an interface.

show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list**command in user EXEC or privileged EXEC mode.

show ipv6 access-list [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of access list.

Command Default

All IPv6 access lists are displayed.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	The priority field was changed to sequence and Layer 4 protocol information (extended IPv6 access list functionality) was added to the display output.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

Examples

The following output from the **show ipv6 access-list**command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Router# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
       left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPSec:

```
Router#  show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
     permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
     permit 89 FE80::/10 any (85 matches) sequence 1
```

The table below describes the significant fields shown in the display.

Table 35: show ipv6 access-list Field Descriptions

Field	Description
ipv6 access list inbound	Name of the IPv6 access list, for example, inbound.
permit	Permits any packet that matches the specified protocol type.
tcp	Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.
any	Equal to ::/0.
eq	An equal operand that compares the source or destination ports of TCP or UDP packets.
bgp	Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to.
reflect	Indicates a reflexive IPv6 access list.

Field	Description
tcptraffic (8 matches)	The name of the reflexive IPv6 access list and the number of matches for the access list. The **clear ipv6 access-list** privileged EXEC command resets the IPv6 access list match counters.
sequence 10	Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80).
host 2001:0DB8:1::1	The source IPv6 host address that the source address of the packet must match.
host 2001:0DB8:1::2	The destination IPv6 host address that the destination address of the packet must match.
11000	The ephemeral source port number for the outgoing connection.
timeout 300	The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session.
(time left 243)	The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds.
evaluate udptraffic	Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound.

Related Commands

Command	Description
clear ipv6 access-list	Resets the IPv6 access list match counters.
hardware statistics	Enables the collection of hardware statistics.
show ip access-list	Displays the contents of all current IP access lists.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

Command	Description
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

show ipv6 cga address-db

To display IPv6 cryptographically generated addresses (CGA) from the address database, use the **show ipv6 cga address-db** command in privileged EXEC mode.

show ipv6 cga address-db

Syntax Description

This command has no arguments or keywords.

Command Default

No CGAs are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example displays CGAs in the CGA database:

```
Router# show ipv6 cga address-db
2001:0DB8:/64 ::2011:B680:DEF4:A550 - table 0x0
        interface:      Ethernet0/0 (3)
        modifier:       SEND1024e
FE80::/64 ::3824:3CE4:C044:8D65 - table 0x12000003
        interface:      Ethernet0/0 (3)
        modifier:       SEND1024e
```

The table below describes the significant fields shown in the display.

Table 36: show ipv6 cga address-db Field Descriptions

Field	Description
2001:0DB8:/64 ::2011:B680:DEF4:A550 - table 0x0	CGA address for which information is shown.
interface:	Interface on which the address is configured.
modifier:	The CGA modifier.

Related Commands

Command	Description
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.

Command	Description
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 cga modifier-db

To display IPv6 cryptographically generated address (CGA) modifier database entries, use the **show ipv6 cga modifier-db** command in privileged EXEC mode.

show ipv6 cga modifier-db

Syntax Description

This command has no arguments or keywords.

Command Default

No CGA modifiers are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 cga modifier-db** command is used to display the modifiers generated with the **ipv6 cga modifier** command and the addresses generated from them.

Examples

The following example displays CGA modifiers in the CGA modifier database:

```
Router# show ipv6 cga modifier-db
F046:E042:13E8:1661:96E5:DD05:94A8:FADC
        label:          SubCA11
        sec level:      1
        Addresses:
  2001:100::38C9:4A1A:2972:794E
  FE80::289C:3308:4719:87F2
```

The table below describes the significant fields shown in the display.

.

Table 37: show ipv6 cga modifier-db Field Descriptions

Field	Description
D695:5D75:F9B5:9715:DF0A:D840:70A2:84B8	The CGA modifier for which the information is displayed.
label	Name used for the Rivest, Shamir, and Adelman (RSA) key pair.
Addresses: 2001:100::38C9:4A1A:2972:794EFE80::289C:3308:4719:87F2	The CGA address.

Related Commands

Command	Description
ipv6 cga modifier	Generates an IPv6 CGA modifier for a specified RSA key pair.
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 inspect

To view Context-based Access Control (CBAC) configuration and session information, use the show ipv6 inspect command in privileged EXEC mode.

show ipv6 inspect {**name inspection-name**| **config**| **interfaces**| **session [detail]**| **all**}

Syntax Description

name *inspection-name*	Displays the configured inspection rule with the name inspection-name.
config	Displays the complete Cisco IOS firewall inspection configuration.
interfaces	Displays interface configuration with respect to applied inspection rules and access lists.
session [**detail**	Displays existing sessions that are currently being tracked and inspected by Cisco IOS firewall. The optional detail keyword causes additional details about these sessions to be shown.
all	Displays all Cisco IOS firewall configuration and all existing sessions that are currently being tracked and inspected by Cisco IOS firewall.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example asks for information about interfaces currently under inspection:

```
Router# show ipv6 inspect
 interfaces
```

Related Commands

Command	Description
ipv6 inspect	Applies a set of inspection rules to an interface.

show ipv6 nd raguard counters

To display information about RA guard counters, use the **show ipv6 nd raguard policy**command in privileged EXEC mode.

show ipv6 nd raguard counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays RA guard policy information for the specified interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(5th)SXI	This command was introduced.

Usage Guidelines

The **show ipv6 nd raguard counters** command displays information about RA guard counters, such as packets sent, packets received, and packets droped. This command also provides information on why a packet was dropped.

show ipv6 nd raguard policy

To display a router advertisements (RAs) guard policy on all interfaces configured with the RA guard feature, use the **show ipv6 nd raguard policy** command in privileged EXEC mode.

show ipv6 nd raguard policy [*policy-name*]

Syntax Description

policy-name	(Optional) RA guard policy name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 nd raguard policy** command displays the options configured for the policy on all interfaces configured with the RA guard feature.

Examples

The following example shows the policy configuration for a policy named raguard1 and all the interfaces where the policy is applied:

```
Router# show ipv6 nd raguard policy interface raguard1

Policy raguard1 configuration:
  device-role host
Policy applied on the following interfaces:
  Et0/0        vlan all
  Et1/0        vlan all
```

The table below describes the significant fields shown in the display.

Table 38: show ipv6 nd raguard policy Field Descriptions

Field	Description
Policy raguard1 configuration:	Configuration of the specified policy.

Field	Description
device-role host	The role of the device attached to the port. This device configuration is that of host.
Policy applied on the following interfaces:	The specified interface on which the RA guard feature is configured.

show ipv6 nd secured certificates

To display active IPv6 Secure Neighbor Discovery (SeND) certificates, use the **show ipv6 nd secured certificates**command in privileged EXEC mode.

show ipv6 nd secured certificates

Syntax Description

This command has no arguments or keywords.

Command Default

No SeND certificates are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured certificates** command is used on hosts (routers configured in host mode) to display the certifcates received over SeND (via Certificate Path Advertisement) and their state.

Examples

The following example displays active SeND certificates:

```
Router# show ipv6 nd secured certificates
Total number of entries: 1 / 32
Hash                             id         RA  certcnt certrcv state
DC0102E09FAF422D49ED79A846D2EBC1 0x00000778 no  1       1       CERT_VALIDATED
certificate No 0
subject  hostname=sa14-72a,c=FR,st=fr,l=example,o=cisco,ou=nsstg,cn=72a
issuer c=FR,st=fr,l=example,o=cisco,ou=nsstg,cn=CA0
```

The table below describes the significant fields shown in the display.

Table 39: show ipv6 nd secured certificates Field Descriptions

Field	Description
certcnt	Number of certificate for this chain.
certrcv	Number of certifciate received in the chain.
Hash	Key hash.
id	Numero of the certifciate.

Field	Description
RA	Displays Yes if an RA is pending for this certifciate.
state	Current state of the certificate.

Related Commands

Command	Description
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 nd secured counters interface

To display IPv6 Secure Neighbor Discovery (SeND) counters on an interface, use the **show ipv6 nd secured counters interface**command in privileged EXEC mode.

show ipv6 nd secured counters interface *interface*

Syntax Description

interface	(Optional) Specifies the interface on which SeND counters are located.

Command Default

No SeND counter information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example displays SeND counters:

```
Router# show ipv6 nd secured counters interface ethernet0/0
e0/0 Received ND messages on Ethernet0/0:
rcvd    accept  SLLA    TLLA    PREFIX  MTU     CGA     RSA     TS      NONCE   TA CERT
RA      66      65      63      0       62      63      63      63      63      0       0
      0
NS      8       8       8       0       0       0       8       8       8       8       0
      0
NA      20      20      0       8       0       0       19      19      19      14      0
      0
CPA     1       1       0       0       0       0       0       0       0       0       1
      1
Dropped ND messages on Ethernet0/0:
Codes   TIMEOUT: Timed out while waiting for rsp
        drop    TIMEOUT
RA      1       1
Sent ND messages on Ethernet0/0:
sent    aborted SLLA    CGA     RSA     TS      NONCE   TA
NS      14      0       14      14      14      14      14      0
NA      8       0       0       8       8       8       8       0
CPS     43      0       0       0       0       0       0       43
Router#
```

The table below describes the significant fields shown in the display.

Table 40: show ipv6 nd secured counters interface Field Descriptions

Field	Description
accept	Number of neighbor discovery (ND) messages accepted (messages that are not dropped).
CERT	Number of messages received with the certificate option.
CGA	Number of messages received with the CGA option.
MTU	Number of messages received with the MTU option.
NA	Number of NDP neighbor advertisements
NONCE	Number of messages received with the NONCE option.
NS	Number of NDP neighbor solicitions.
PREFIX	Number of messages received with the PREFIX option.
rcvd	Number of ND messages received on the interface.
RA	Number of router advertisements.
REDIR	Number of NDP redirect messages.
RS	Router Solicit.
RSA	Number of messages received with the RSA option.
SLLA	Number of messages received with the ND SLLA option.
TA	Number of messages received with the trust anchor option.
TS	Number of messages received with the time stamp option.

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.

Command	Description
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND timestamp entries.

show ipv6 nd secured nonce-db

To display active IPv6 Secure Neighbor Discovery (SeND) nonce database entries, use the **show ipv6 nd secured nonce-db**command in privileged EXEC mode.

show ipv6 nd secured nonce-db

Syntax Description

This command has no arguments or keywords.

Command Default

No SeND nonce information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured nonce-db**command is used to display the pending solicitations. There are rarely any pending solicitations because the solicitations are quickly answered and removed from the database.

Examples

The following example displays active SeND nonce entries. The output is self-explanatory.

```
Router# show ipv6 nd secured nonce-db
Total number of entries: 0
```

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured timestamp-db	Displays active SeND time stamp entries.

show ipv6 nd secured solicit-db

To display pending SEcure Neighbor Discovery (SEND) solicitations from peers, use the **show ipv6 nd secured solicit-db**command in privileged EXEC configuration mode.

show ipv6 nd secured solicit-db

Syntax Description

This command has no arguments or keywords.

Command Default

No pending SEND solicitation information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use this command to display pending SEND solicitations.

Examples

The following example displays pending SEcure Neighbor Discovery (SEND) solicitations from peers:

```
Router# show ipv6 nd secured solicit-db
```

show ipv6 nd secured timestamp-db

To display active Secure Neighbor Discovery (SeND) time-stamp database entries, use the **show ipv6 nd secured timestamp-db**command in privileged EXEC mode.

show ipv6 nd secured timestamp-db

Syntax Description

This command has no arguments or keywords.

Command Default

No pending SeND solicitation information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured timestamp-db** command displays the content of the time-stamp databse, which contains last received messages from peers. It also displays the delta and fuzz values.

Examples

The following example displays active SeND time-stamp database entries:

```
Router# show ipv6 nd secured timestamp-db
Total number of entries: 6 Number of unreached peer entries: 3 / 1024
FE80::289C:3308:4719:87F2 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 41m 16s (reached)
        TSlast: 0x4936B97655FF = Wed Dec  3 16:53:10 2008
        RDlast: 0x4936B976438B = Wed Dec  3 16:53:10 2008
FE80::2441:88D1:22FC:3B77 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 59m 53s (reached)
        TSlast: 0x4936BDD2E13E = Wed Dec  3 17:11:46 2008
        RDlast: 0x4936BDD2D0D6 = Wed Dec  3 17:11:46 2008
FE80::E2:F012:6F72:9E45 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 18s (unreached)
        TSlast: 0x4936B0CBB333 = Wed Dec  3 16:16:11 2008
        RDlast: 0x4936B0CBBD70 = Wed Dec  3 16:16:11 2008 2001:100::38C9:4A1A:2972:794E on
 Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 19s (unreached)
        TSlast: 0x4936BA254FDA = Wed Dec  3 16:56:05 2008
        RDlast: 0x4936BA253F72 = Wed Dec  3 16:56:05 2008 2001:100::383E:6BD5:397:4A50 on
Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 45m 0s (reached)
        TSlast: 0x4936BA55F2AA = Wed Dec  3 16:56:53 2008
        RDlast: 0x4936BA55E036 = Wed Dec  3 16:56:53 2008
2001:100::434:E62D:327D:B1E6 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 42s (unreached)
        TSlast: 0x4936B0E422D0 = Wed Dec  3 16:16:36 2008
        RDlast: 0x4936B0E42D0E = Wed Dec  3 16:16:36 2008
```

The table below describes the significant fields shown in the display.

Table 41: show ipv6 nd secured timestamp-db Field Descriptions

Field	Description
Total number of entries	Number of entries (peers) in the cache.
Time to expire	Remaining time before entry expires.
TSlast	Last peer timestamp value.
RDlast	Time when the last message was received from the peer.

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.

show ipv6 port-map

To verify port-to-application mapping (PAM) configuration, use the **show ipv6 port-map**command in user EXEC or privileged EXEC mode.

show ipv6 port-map [*application*| **port** *port-number*]

Syntax Description

application	(Optional) Specifies the name of the application used in port mapping.
port *port-number*	(Optional) Specifies the port number that maps to the application.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **show ipv6 port-map** command displays the entire IPv6 port-mapping table or specific port-mapping information of a particular port number or application (protocol). Enabling the **show ipv6 port-map** command displays the entire IPv6 PAM table, including system-defined, user-defined, and host-specific port-mapping configurations.

To display port-mapping details of a specific port number, use the **show ipv6 port-map** command with the **port***port-number* keyword and argument.

To display the port-mapping details of a specific application, use the **show ipv6 port-map** command with the *application* argument.

Examples

The following example displays the FTP application's PAM information:

```
Router# show ipv6 port-map ftp
```

The following example displays PAM information at port number 21:

```
Router# show ipv6 port-map port 21
```

Related Commands

Command	Description
ipv6 port-map	Establishes PAM for the system.

show ipv6 prefix-list

To display information about an IPv6 prefix list or IPv6 prefix list entries, use the **show ipv6 prefix-list**command in user EXEC or privileged EXEC mode.

show ipv6 prefix-list [**detail**| **summary**] [*list-name*]

show ipv6 prefix-list *list-name ipv6-prefix/prefix-length* [**longer**| **first-match**]

show ipv6 prefix-list *list-name* **seq** *seq-num*

Syntax Description

detail | **summary**	(Optional) Displays detailed or summarized information about all IPv6 prefix lists.
list-name	(Optional) The name of a specific IPv6 prefix list.
ipv6-prefix	All prefix list entries for the specified IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. 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.
longer	(Optional) Displays all entries of an IPv6 prefix list that are more specific than the given *ipv6-prefix* / *prefix-length*values.
first-match	(Optional) Displays the entry of an IPv6 prefix list that matches the given *ipv6-prefix* / *prefix-length*values.
seq *seq-num*	The sequence number of the IPv6 prefix list entry.

Command Default

Displays information about all IPv6 prefix lists.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.

Release	Modification
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show ipv6 prefix-list** command provides output similar to the **show ip prefix-list** command, except that it is IPv6-specific.

Examples

The following example shows the output of the **show ipv6 prefix-list** command with the **detail** keyword:

```
Router# show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
   seq 5 permit 2002::/16 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
   seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
   seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
   seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
   seq 10 deny ::/0 (hit count: 0, refcount: 1)
   seq 15 deny ::/1 (hit count: 0, refcount: 1)
   seq 20 deny ::/2 (hit count: 0, refcount: 1)
   seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
   seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

The table below describes the significant fields shown in the display.

Table 42: show ipv6 prefix-list Field Descriptions

Field	Description
Prefix list with the latest deletion/insertion:	Prefix list that was last modified.
count	Number of entries in the list.
range entries	Number of entries with matching range.
sequences	Sequence number for the prefix entry.
refcount	Number of objects currently using this prefix list.

Field	Description
seq	Entry number in the list.
permit, deny	Granting status.
hit count	Number of matches for the prefix entry.

The following example shows the output of the **show ipv6 prefix-list** command with the **summary**keyword:

```
Router# show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

Related Commands

Command	Description
clear ipv6 prefix-list	Resets the hit count of the prefix list entries.
distribute-list in	Filters networks received in updates.
distribute-list out	Suppresses networks from being advertised in updates.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 prefix-list description	Adds a text description of an IPv6 prefix list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
remark (prefix-list)	Adds a comment for an entry in a prefix list.

show ipv6 snooping capture-policy

To display message capture policies, use the **show ipv6 snooping capture-policy** command in user EXEC or privileged EXEC mode.

show ipv6 snooping capture-policy [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first-hop message types on the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The **show ipv6 snooping capture-policy** command displays IPv6 first-hop message capture policies.

Examples

The following example shows **show ipv6 snooping capture-policy** command output on the Ethernet 0/0 interface, on which the IPv6 Neighbor Discovery Protocol (NDP) Inspection and Router Advertisement (RA) Guard features are configured:

```
Router# show ipv6 snooping capture-policy

Hardware policy registered on Et0/0
Protocol  Protocol value  Message  Value  Action  Feature
ICMP      58              RS       85     punt    RA Guard
                                          punt    ND Inspection
ICMP      58              RA       86     drop    RA guard
                                          punt    ND Inspection
ICMP      58              NS       87     punt    ND Inspection
ICMP      58              NA       88     punt    ND Inspection
ICMP      58              REDIR    89     drop    RA Guard
                                          punt    ND Inspection
```

The table below describes the significant fields shown in the display.

Table 43: show ipv6 snooping capture-policy Field Descriptions

Field	Description
Hardware policy registered on Fa4/11	A hardware policy contains a programmatic access list (ACL), with a list of access control entries (ACEs).
Protocol	The protocol whose packets are being inspected.
Message	The type of message being inspected.
Action	Action to be taken on the packet.
Feature	The inspection feature for this information.

show ipv6 snooping counters

To display information about the packets counted by the interface counter, use the **show ipv6 snooping counters**command in user EXEC or privileged EXEC mode.

show ipv6 snooping counters {**interface** *type number*| **vlan** *vlan-id*}

Syntax Description

interface *type number*	Displays first-hop packets that match the specified interface type and number.
vlan *vlan-id*	Displays first hop packets that match the specified VLAN ID.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The **show ipv6 snooping counters** command displays packets handled by the switch that are being counted in interface counters. The switch counts packets captured per interface and records whether the packet was received, sent, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.

Examples

The following examples shows information about packets counted on Fast Ethernet interface 4/12:

```
Router# show ipv6 snooping counters interface Fa4/12
Received messages on Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4256    0       0       0       0       0
Bridged messages from Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
```

```
               0       4240    0       0       0       0       0
Dropped messages on Fa4/12:
Feature/Message RS      RA      NS      NA      REDIR   CPS     CPA
RA guard        0       16      0       0       0       0       0
Dropped reasons on Fa4/12:
RA guard         16   RA drop - reason:RA/REDIR received on un-authorized port
```

The table below describes the significant fields shown in the display.

Table 44: show ipv6 snooping counters Field Descriptions

Field	Description
Received messages on:	The messages received on an interface.
Protocol	The protocol for which messages are being counted.
Protocol message	The type of protocol messages being counted.
Bridged messages from:	Bridged messages from the interface.
Dropped messages on:	The messages dropped on the interface.
Feature/message	The feature that caused the drop, and the type and number of messages dropped.
RA drop - reason:	The reason that these messages were dropped.

show ipv6 snooping features

To display information about about snooping features configured on the router, use the **show ipv6 snooping features** command in user EXEC or privileged EXEC mode.

show ipv6 snooping features

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The **show ipv6 snooping features** command displays the first-hop features that are configured on the router.

Examples

The following example shows that both IPv6 NDP inspection and IPv6 RA guard are configured on the router:

```
Router# show ipv6 snooping features

Feature name   priority state
RA guard          100   READY
NDP inspection     20   READY
```

The table below describes the significant fields shown in the display.

Table 45: show ipv6 snooping features Field Descriptions

Field	Description
Feature name	The names of the IPv6 global policy features configured on the router.
priority	The priority of the specified feature.
state	The state of the specified feature.

show ipv6 snooping policies

To display information about the configured policies and the interfaces to which they are attached, use the **show ipv6 snooping policies** command in user EXEC or privileged EXEC mode.

show ipv6 snooping policies {**interface** *type number*| **vlan** *vlan-id*}

Syntax Description

interface *type number*	Displays policies that match the specified interface type and number.
vlan *vlan-id*	Displays first-hop packets that match the specified VLAN ID.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The **show ipv6 snooping policies** command displays all policies that are configured and lists the interfaces to which they are attached.

Examples

The following example shows information about all policies configured:

```
Device# show ipv6 snooping policies

NDP inspection policies configured:
Policy      Interface    Vlan
------      ---------    ----
trusted      Et0/0        all
             Et1/0        all
untrusted    Et2/0        all
RA guard policies configured:
Policy      Interface    Vlan
------      ---------    ----
host         Et0/0        all
             Et1/0        all
router       Et2/0        all
```

The table below describes the significant fields shown in the display.

Table 46: show ipv6 snooping policies Field Descriptions

Field	Description
NDP inspection policies configured:	Description of the policies configured for a specific feature.
Policy	Whether the policy is trusted or untrusted.
Interface	The interface to which a policy is attached.

show ipv6 spd

To display the IPv6 Selective Packet Discard (SPD) configuration, use the **show ipv6 spd**command in privileged EXEC mode.

show ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Use the **show ipv6 spd** command to display the SPD configuration, which may provide useful troubleshooting information.

Examples

The following is sample output from the **show ipv6 spd** command:

```
Router# show ipv6 spd
Current mode: normal
Queue max threshold: 74, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0
```

The table below describes the significant fields shown in the display.

Table 47: show ipv6 spd Field Description

Field	Description
Current mode: normal	The current SPD state or mode.
Queue max threshold: 74	The process input queue maximum.

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the SPD process input queue.

show ipv6 virtual-reassembly

To display Virtual Fragment Reassembly (VFR) configuration and statistical information on a specific interface, use the **show ipv6 virtual-reassembly** command in privileged EXEC mode.

show ipv6 virtual-reassembly interface *interface-type*

Syntax Description

interface *interface-type*	Specifies the interface for which information is requested.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

This command shows the configuration and statistical information of VFR on the given interface.

Examples

The following example shows a typical display produced by this command:

```
Router# show ipv6 virtual-reassembly
All enabled IPv6 interfaces...
GigabitEthernet0/0/0:
   IPv6 Virtual Fragment Reassembly (IPV6VFR) is ENABLED [in]
   IPv6 configured concurrent reassemblies (max-reassemblies): 64
   IPv6 configured fragments per reassembly (max-fragments): 16
   IPv6 configured reassembly timeout (timeout): 3 seconds
   IPv6 configured drop fragments: OFF

   IPv6 current reassembly count:0
   IPv6 current fragment count:0
   IPv6 total reassembly count:20
   IPv6 total reassembly timeout count:0
```

The display is self-explanatory; it corresponds to the values used when you entered the **ipv6 virtual-reassembly** command.

Related Commands

Command	Description
ipv6 virtual-reassembly	Enables VFR on an interface.

show ipv6 virtual-reassembly features

To display Virtual Fragment Reassembly (VFR) information on all interfaces or on a specified interface, use the **show ipv6 virtual-reassembly features** command in privileged EXEC mode.

show ipv6 virtual-reassembly features [**interface** *interface-type*]

Syntax Description

interface *interface-type*	(Optional) Specifies the interface for which information is requested.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

This command shows the configuration and statistical information of VFR on a specified interface or on all interfaces. Use the optional **interface** *interface-type* keyword and argument to specify an interface. If you enter the **show ipv6 virtual-reassembly features** command without the keyword and argument, information about all interfaces is displayed.

Examples

The following example displays information about all interfaces:

```
Router# show ipv6 virtual-reassembly features

GigabitEthernet0/0/0:
  IPV6 Virtual Fragment Reassembly (IPV6 VFR) Current Status is ENABLED [in]
  Features to use if IPV6 VFR is Enabled:CLI
GigabitEthernet0/0/0:
  IPV6 Virtual Fragment Reassembly (IPV6 VFR) Current Status is ENABLED [out]
  Features to use if IPV6 VFR is Enabled:CLI
```

The display is self-explanatory; it corresponds to the values used when you entered the **ipv6 virtual-reassembly** command.

Related Commands

Command	Description
ipv6 virtual-reassembly	Enables VFR on an interface.
show ipv6 virtual-reassembly	Displays VFR configuration and statistical information.

show kerberos creds

To display the contents of your credentials cache, use the **show kerberos creds** command in privileged EXEC mode.

show kerberos creds

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show kerberos creds** command is equivalent to the UNIX klist command.

When users authenticate themselves with Kerberos, they are issued an authentication ticket called a *credential* . The credential is stored in a credential cache.

Examples

The following example displays entries in the credentials cache:

```
Router > show kerberos creds

 Default Principal: user@example.com
 Valid Starting          Expires                 Service Principal
 18-Dec-1995 16:21:07    19-Dec-1995 00:22:24    krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

The following example returns output that acknowledges that credentials do *not* exist in the credentials cache:

```
Router > show kerberos creds
 No Kerberos credentials
```

Related Commands

Command	Description
clear kerberos creds	Deletes the contents of the credentials cache.

show ldap attributes

To display attributes of the Lightweight Directory Access Protocol (LDAP) server, use the **show ldap attributes**command in user EXEC or privileged EXEC mode.

show ldap attributes

Syntax Description

This command has no arguments and keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use the **show ldap attributes** command to display the default mapping of LDAP attributes to AAA attributes. It displays the dynamic attribute map that is configured on the router.

Examples

The followingis sample output from the **show ldap server** command:

```
Router# show ldap attributes
LDAP Attribute                    Format      AAA Attribute
==============                    ======      =============
airespaceBwDataBurstContract     Ulong       bsn-data-bandwidth-burst-contr
userPassword                     String      password
airespaceBwRealBurstContract     Ulong       bsn-realtime-bandwidth-burst-c
employeeType                     String      employee-type
airespaceServiceType             Ulong       service-type
airespaceACLName                 String      bsn-acl-name
priv-lvl                         Ulong       priv-lvl
memberOf                         String DN   supplicant-group
cn                               String      username
airespaceDSCP                    Ulong       bsn-dscp
policyTag                        String      tag-name
airespaceQOSLevel                Ulong       bsn-qos-level
airespace8021PType               Ulong       bsn-8021p-type
airespaceBwRealAveContract       Ulong       bsn-realtime-bandwidth-average
airespaceVlanInterfaceName       String      bsn-vlan-interface-name
airespaceVapId                   Ulong       bsn-wlan-id
airespaceBwDataAveContract       Ulong       bsn-data-bandwidth-average-con
sAMAccountName                   String      sam-account-name
meetingContactInfo               String      contact-info
telephoneNumber                  String      telephone-number
Map: att_map_1
department                       String DN   element-req-qos
```

The table below describes the significant fields shown in the display.

Table 48: show ldap attributes Descriptions

Field	Description
LDAP Attribute	LDAP distinguished name attribute (or attributes).
Format	Format conversion of the attribute.
AAA Attribute	Authentication, Authorization, and Accounting (AAA) distinguished name attribute (or attributes).

Related Commands

Command	Description
attribute-map	Attaches an attribute map to a particular LDAP server.
ldap attribute-map	Configures a dynamic LDAP attribute map.
map-type	Defines the mapping of an attribute in the LDAP server.
show ldap server	Displays properties of the LDAP server.

show ldap server

To display properties of the Lightweight Directory Access Protocol (LDAP) server, use the **show ldap server** command in user EXEC or privileged EXEC mode.

show ldap server {*name* | **all**} {**connections** | **statistics** | **summary**}

Syntax Description

name	The name of the configured LDAP server for which to display the properties.
all	Displays properties for all LDAP servers.
connections	Displays the number of connections to the LDAP server.
statistics	Displays the LDAP statistics.
summary	Displays the LDAP server information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.2(2)T	This command was modified. The **connections**, **statistics**, and **summary** keywords were added.

Examples

The following is sample output from the **show ldap server** command:

```
Device# show ldap server ldap1 connections

Sock  Connection Status   Root Bind Status
---------------------------------------------
0     UP                  Root-dn Bind Done
No. of active connections   :1


Device# show ldap server ldap1 statistics

---------------------------------
* LDAP STATISTICS *
Total messages  [Sent:3, Received:7]
Response delay(ms) [Average:543, Maximum:581]
Total search    [Request:1, ResultEntry:4, ResultDone:1]
```

```
Total bind      [Request:2, Response:2]
Total extended  [Request:0, Response:0]
Total compare   [Request:0, Response:0]
Search [Success:1, Failures:0]
Bind   [Success:2, Failures:0]
Missing attrs in Entry [0]
---------------------------------

Device# show ldap server ldap1 summary

Server Information for ldap1
================================
Server name             :ldap1
Server IP               :10.64.67.66
Server listening Port   :389
Bind Root-dn            :cn=admin,dc=ldap,dc=com
Server mode             :Non-Secure
Secure Trustpoint       :MSCA1
Cipher Suite            :0x00
Authentication Seq      :Bind/Compare password first. Search next
Authentication Procedure:Bind with user password
Base-Dn                 :dc=ldap,dc=com
Request timeout         :30
No. of active connections   :1
---------------------------------

Device# show ldap server all

Server Information for ldap1
================================
Server name              :ldap1
Server Address           :2001:DB8:0:0:8:800
Server listening Port    :389
Bind Root-dn             :cn=iosadmin,dc=aaaldap,dc=com
Server mode              :Non-Secure
Cipher Suite             :0x00
Authentication Seq       :Bind/Compare password first. Search next
Authentication Procedure :Bind with user password
Base-Dn                  :dc=aaaldap,dc=com
Object Class             :top
Request timeout          :30
---------------------------------
* LDAP STATISTICS *
Total messages  [Sent:0, Received:0]
Response delay(ms) [Average:0, Maximum:0]
Total search    [Request:0, ResultEntry:0, ResultDone:0]
Total bind      [Request:0, Response:0]
Total extended  [Request:0, Response:0]
Total compare   [Request:0, Response:0]
Search [Success:0, Failures:0]
Bind   [Success:0, Failures:0]
Missing attrs in Entry [0]
---------------------------------
No. of active connections   :0
---------------------------------
```

The following table describes the significant fields shown in the display.

Table 49: show ldap server Field Descriptions

Field	Description
No. of active connections	Total number of connections to the LDAP server.
Total messages	Total number of sent and received LDAP messages.
Response delay (ms)	Maximum and average delay in response, in milliseconds.

Field	Description
Total search	Total number of search requests and results for directory entries.
Total bind	Total number of user credentials verified with the LDAP server.
Total extended	Total number of Transport Layer Security (TLS) extension operations.
Total compare	Total number of requests and results to find if a named entry contains a given attribute value.
Search	Number of successful and failed user search results for directory entries.
Bind	Number of successful and failed user authentication entries.
Missing attrs in Entry	Number of missing attributes in an LDAP entry. LDAP entries contain multiple attributes received from the LDAP server.
Server name	LDAP server name.
Server IP	IP address of the LDAP server.
Server Address	IPv6 address of the LDAP server.
Server listening Port	The transport layer port on which the server is listening.
Bind Root-dn	Distinguished name of the LDAP server.
Server mode	Security mode.
Secure Trustpoint	Secure LDAP server name.
Cipher Suite	Cryptographic algorithms used in the connection.
Authentication Seq	LDAP authentication sequence.
Authentication Procedure	Authentication method.
Base-Dn	Distinguished name of the search base.
Request timeout	Response timeout. The default timeout value is 30 seconds.

Related Commands

Command	Description
show ldap attribute	Displays information about default LDAP attribute mapping.

show logging ip access-list

To display information about the logging IP access list, use the **show logging ip access-list**command in privileged EXEC mode.

show logging ip access-list {**cache**| **config**}

Syntax Description

cache	Displays information about all the entries in the Optimized ACL Logging (OAL) cache.
config	Displays information about the logging IP access-list configuration.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to include the **config** keyword on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

OAL is supported on IPv4 unicast traffic only.

Examples

This example shows how to display all the entries in the OAL cache:

```
Router# show logging ip access-list cache
Matched flows:
id prot src_ip dst_ip sport dport status count
total lastlog
-------------------------------------------------------------------------------------
1 17 10.2.1.82 10.2.12.2 111 63 Permit 0
3906 2d02h
2 17 10.2.1.82 10.2.12.2 1135 63 Permit 0
3906 2d02h
3 17 10.2.1.82 10.2.12.2 2159 63 Permit 0
3906 2d02h
```

```
4 17 10.2.1.82 10.2.12.2 3183 63 Permit 0
3906 2d02h
5 17 10.2.1.82 10.2.12.2 4207 63 Permit 0
3906 2d02h
6 17 10.2.1.82 10.2.12.2 5231 63 Deny 0
3906 2d02h
7 17 10.2.1.82 10.2.12.2 6255 63 Deny 0
3906 2d02h
8 17 10.2.1.82 10.2.12.2 7279 63 Permit 0
3906 2d02h
9 17 10.2.1.82 10.2.12.2 8303 63 Permit 0
3906 2d02h
10 17 10.2.1.82 10.2.12.2 9327 63 Permit 0
3905 2d02h
11 17 10.2.1.82 10.2.12.2 10351 63 Permit 0
3905 2d02h
12 17 10.2.1.82 10.2.12.2 11375 63 Permit 0
3905 2d02h
13 17 10.2.1.82 10.2.12.2 12399 63 Deny 0
3905 2d02h
14 17 10.2.1.82 10.2.12.2 13423 63 Permit 0
3905 2d02h
15 17 10.2.1.82 10.2.12.2 14447 63 Deny 0
3905 2d02h
16 17 10.2.1.82 10.2.12.2 15471 63 Permit 0
3905 2d02h
17 17 10.2.1.82 10.2.12.2 16495 63 Permit 0
3905 2d02h
18 17 10.2.1.82 10.2.12.2 17519 63 Permit 0
3905 2d02h
19 17 10.2.1.82 10.2.12.2 18543 63 Permit 0
3905 2d02h
20 17 10.2.1.82 10.2.12.2 19567 63 Permit 0
3905 2d02h
Number of entries: 20
Number of messages logged: 112
Number of packets logged: 11200
Number of packets received for logging: 11200
```

This example shows how to display information about the logging IP access-list configuration:

```
Router# show logging ip access-list config
Logging ip access-list configuration
 Maximum number of cached entries: 8192
 Logging rate limiter: 0
 Log-update interval: 300
 Log-update threshold: 0
 Configured on input direction:
        Vlan2
        Vlan1
 Configured on output direction:
        Vlan2
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (global configuration)	Configures the OAL parameters.
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.

show login

To display login parameters, use the **show login**command in privileged EXEC mode.

show login [failures]

Syntax Description

failures	(Optional) Displays information related only to failed login attempts.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show login**command allows users to verify the applied login configuration and present login status on your router.

Examples

The following sample output from the **show login** command verifies that no login parameters have been specified:

```
Router# show login
No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps
Router NOT enabled to watch for login Attacks
```

The following sample output from the **show login** command verifies that the **login block-for**command is issued. In this example, the command is configured to block login hosts for 100 seconds if 16 or more login requests fail within 100 seconds; 5 login requests have already failed.

```
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
```

```
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

The following sample output from the **show login** command verifies that the router is in quiet mode. In this example, the **login block-for** command was configured to block login hosts for 100 seconds if 3 or more login requests fail within 100 seconds.

```
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100
 seconds.
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
```

Denying logins from all sources.

The table below describes the significant fields shown in the proceeding displays.

Table 50: show login Field Descriptions

Field	Description
A default login delay of 1 seconds is applied.	A delay of 1 second is enforced when the **login block-for** command is issued. To specify a different delay value, use the **login delay** command.
No Quiet-Mode access list has been configured.	No access control lists (ACLs) are exempt from the quiet period. To specify an ACL, use the **login quiet-mode access-class** command.
All successful or failed login is logged and generate SNMP traps.	Logging messages and Simple Network Management Protocol (SNMP) traps are configured to be generated upon successful or failed login attempts. To change this setting, use the **login on-success** or **login on-failure** command.
Router enabled to watch for login Attacks.	The Cisco IOS device has been configured with at least the **login block-for** command, which enables default login functionality. **Note** If no login parameters are specified, the following description appears: " Router NOT enabled to watch for login Attacks . "

Field	Description
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100 seconds.	Parameters of the **login block-for** *seconds* **attempts** *tries* **within** *seconds* command.
`Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.`	The router has switched to quiet mode. **Note** If the router is not in quiet mode, the following description appears: " Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds."
Denying logins from all sources.	The router is in quiet mode and no ACLs are defined, so the router is denying all login requests. **Note** If the router is not in quiet mode, the following description, which allows the user to keep track of the current failed login attempts, appears: "Present login failure count 5."

Examples

The following sample output from **show login failures** command shows all failed login attempts on the router:

```
Router# show login failures
Information about login failure's with the device
Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Mar 9 2003
try2          10.1.1.2        23    1     21:52:52 UTC Sun Mar 9 2003
```

The following sample output from **show login failures** command verifies that no information is presently logged:

```
Router# show login failures
*** No logged failed login attempts with the device.***
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
login delay	Configures a uniform delay between successive login attempts.
login on-failure	Generates system logging messages for every login attempts.
login on-success	Generates system logging messages for successful login attempts.
login quiet-mode access-class	Specifies an ACL that is to be applied to the router when it switches to quiet mode.

show mab

To display MAC Authentication Bypass (MAB) information, use the **show mab** command in privileged EXEC mode.

show mab {**all**| **interface** *type number*} **[detail]**

Syntax Description

all	Specifies all interfaces.
interface *type number*	Specifies a particular interface for which to display MAB information.
detail	(Optional) Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
15.2(3)T	This command was modified. The authorization status of the authentication result is displayed as SUCCESS or FAIL instead of AUTHORIZED or UNAUTHORIZED in the command output.

Usage Guidelines

Use the **show mab** command to display information about MAB ports and MAB sessions.

Examples

The following is sample output from the **show mab interface detail** command where a MAB session has been authorized:

```
Switch# show mab interface
FastEthernet1/0/1
 detail
MAB details for FastEthernet1/0/1
-----------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
MAB Client List
---------------
Client MAC                = 000f.23c4.a401
MAB SM state              = TERMINATE
Auth Status               = SUCCESS
```

The table below describes the significant fields shown in the display.

Table 51: show mab Field Descriptions

Field	Description
Mac-Auth-Bypass	Specifies whether MAB is enabled or disabled.
Inactivity Timeout	The period of time of no activity after which the session is ended.
Client MAC	The MAC address of the client.
MAB SM state	The state of the MAB state machine. The possible values, from start to finish, are: • INITIALIZE--the state of the session when it is being initialized. • ACQUIRING--the state of the session when the MAC address is being obtained from the client. • AUTHORIZING--the state of the session when the MAC address is being authorized. • TERMINATE--the state of the session once an authorization result has been obtained.
Auth Status	The authorization status of the MAB session. The possible values are: • SUCCESS--the session has been successfully authorized. • FAIL--the session failed to be authorized.

Related Commands

Command	Description
show authentication interface	Displays information about the Auth Manager for a given interface.
show authentication registrations	Displays information about authentication methods registered with the Auth Manager.
show authentication sessions	Displays information about Auth Manager sessions.

show mac access-group interface

To display the ACL configuration on a Layer 2 interface, use the **show mac access-group interface**command.

show mac access-group interface [*interface interface-number*]

Syntax Description

interface	(Optional) Specifies the interface type; valid values are **gigabitethernet**, **tengigabitethernet**, **longreachethernet**, and **port-channel**.
interface-number	(Optional) Specifies the port number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXH	Support for this command was introduced.
12.2(33)SRB	Support for this command was introduced.
12.2(33)SRD3	Support for this command was introduced.

Usage Guidelines

The valid values for the port number depend on the chassis used.

Examples

This example shows how to display the ACL configuration on interface fast 6/1:

```
Switch# show mac access-group interface gigabitethernet 6/1
Interface FastEthernet6/1:
   Inbound access-list is simple-mac-acl
   Outbound access-list is not set
```

Related Commands

Command	Description
access-group mode	Specifies the override modes (for example, VACL overrides PACL) and the non-override modes (for example, merge or strict mode).

show mac-address-table

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

Cisco 2600, 3600, and 3700 Series Routers

show mac-address-table [**secure**| **self**| **count**][**address***macaddress*][**interface***type/number*]{**fa** | **gi***slot/port*}[**atm***slot/port*][**atm***slot/port*][**vlan***vlan-id*]

Catalyst 4500 Series Switches

show mac-address-table {**assigned**| **ip**| **ipx**| **other**}

Catalyst 6000/6500 Series Switches and 7600 Series Routers

show mac-address-table [**address** *mac-addr* [**all** | **interface** *type/number* | **module** *number* | **vlan** *vlan-id*] | **aging-time** [**vlan** *vlan-id*] | **count**[**module** *number* | **vlan** *vlan-id*] | **interface** *type/number* | **limit** [**vlan** *vlan-id* | **module** *number* | **interface** *type*] | **module** *number* | **multicast** [**count**] [**igmp-snooping** | **mld-snooping** | **user**][**vlan** *vlan-id*] | **notification** {**mac-move**[**counter**[**vlan**]]| **threshold**| **change**}[**interface** [*number*]] | **synchronize statistics** | **unicast-flood** | **vlan** *vlan-id* [**all**| **module** *number*]]

Syntax Description

secure	(Optional) Displays only the secure addresses.
self	(Optional) Displays only addresses added by the switch itself.
count	(Optional) Displays the number of entries that are currently in the MAC address table.
address *mac-addr*	(Optional) Displays information about the MAC address table for a specific MAC address. See the Usage Guidelines section for formatting information.
interface *type* / *number*	(Optional) Displays addresses for a specific interface. For the Catalyst 6500 and 6000 series switches, valid values are **atm**, **fastethernet**, **gigabitethernet**, and **port-channel**. For the Cisco 7600 series, valid values are **atm**,**ethernet**, **fastethernet**, **ge-wan**, **gigabitethernet**, **tengigabitethernet**, and **pos**.
fa	(Optional) Specifies the Fast Ethernet interface.
gi	(Optional) Specifies the Gigabit Ethernet interface.
slot / *port*	(Optional) Adds dynamic addresses to the module in slot 1 or 2. The slash mark is required.

atm *slot /port*	(Optional) Adds dynamic addresses to ATM module *slot /port* . Use 1 or 2 for the slot number. Use 0 as the port number. The slash mark is required.
vlan *vlan -id*	(Optional) Displays addresses for a specific VLAN. For the Cisco 2600, 3600, and 3700 series, valid values are from 1 to 1005; do not enter leading zeroes. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094. For the Catalyst 6500 and 6000 series switches and 7600 series, valid values are from 1 to 4094.
assigned	Specifies the assigned protocol entries.
ip	Specifies the IP protocol entries.
ipx	Specifies the IPX protocol entries.
other	Specifies the other protocol entries.
all	(Optional) Displays every instance of the specified MAC address in the forwarding table.
type / *number*	(Optional) Module and interface number.
module *number*	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.
aging-time	(Optional) Displays the aging time for the VLANs.
limit	Displays MAC-usage information.
multicast	Displays information about the multicast MAC address table entries only.
igmp-snooping	Displays the addresses learned by Internet Group Management Protocol (IGMP) snooping.
mld-snooping	Displays the addresses learned by Multicast Listener Discover version 2 (MLDv2) snooping.
user	Displays the manually entered (static) addresses.
notification mac-move	Displays the MAC-move notification status.
notification mac-move counter	(Optional) Displays the number of times a MAC has moved and the number of these instances that have occurred in the system.

vlan	(Optional) Specifies a VLAN to display. For the Catalyst 6500 and 6000 series switches and 7600 series, valid values are from 1 to 4094.
notification threshold	Displays the Counter-Addressable Memory (CAM) table utilization notification status.
notification change	Displays the MAC notification parameters and history table.
synchronize statistics	Displays information about the statistics collected on the switch processor or DFC.
unicast-flood	Displays unicast-flood information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2(8)SA	This command was introduced.
11.2(8)SA3	This command was modified. The **aging-time** ,, **count**, **self** , and **vlan** *vlan-id* keywords and arguments were added.
11.2(8)SA5	This command was modified. The **atm***slot*/*port* keyword-argument pair was added.
12.2(2)XT	This command was modified. This command was implemented on Cisco 2600, 3600, and 3700 series routers.
12.1(8a)EW	This command was modified. This command was implemented on Catalyst 4500 series switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600, 3600, and 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(14)SX	This command was modified. This command was implemented on the Supervisor Engine 720.

Release	Modification
12.2(17a)SX	This command was modified. For the Catalyst 6500 and 6000 series switches and 7600 series, this command was changed to support the following optional keywords and arguments: • **count module** *number* • **limit** [**vlan** *vlan-id* | **port** *number* | **interface** *interface-type* • **notification threshold** • **unicast-flood**
12.2(17d)SXB	This command was modified. Support for this command was added for the Supervisor Engine 2.
12.2(18)SXE	This command was modified. For the Catalyst 6500 and 6000 series switches and Cisco 7600 series, support was added for the **mld-snooping** keyword on the Supervisor Engine 720 only.
12.2(18)SXF	This command was modified. For the Catalyst 6500 and 6000 series switches and Cisco 7600 series, support was added for the **synchronizestatistics** keywords on the Supervisor Engine 720 only.
12.2(33)SRA	This command was modified. This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs to 1 to 4094 for specified platforms.
12.2(33)SXH	This command was modified. The **change** keyword was added.
12.2(33)SXI	This command was modified to add the **counter** keyword.

Usage Guidelines

Cisco 2600, 3600, and 3700 Series Routers

The **show mac-address-table** command displays the MAC address table for the switch. Specific views can be defined by using the optional keywords and arguments. If more than one optional keyword is used, then all the conditions must be true for that entry to be displayed.

Catalyst 4500 Series Switches

For the MAC address table entries that are used by the routed ports, the routed port name, rather than the internal VLAN number, is displayed in the □vlan□ column.

Catalyst 6000 and 6500 Series Switches and Cisco 7600 Series Routers

If you do not specify a module number, the output of the **show mac-address-table** command displays information about the supervisor engine. To display information about the MAC address table of the DFCs, you must enter the module number or the **all** keyword.

The *mac-addr*value is a 48-bit MAC address. The valid format is H.H.H.

The interface *number* argument designates the module and port number. Valid values depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The optional **module** *number* keyword-argument pair is supported only on DFC modules. The **module** *number*keyword-argument pair designate the module number.

Valid values for the *mac-group-address* argument are from 1 to 9.

The optional **count** keyword displays the number of multicast entries.

The optional **multicast** keyword displays the multicast MAC addresses (groups) in a VLAN or displays all statically installed or IGMP snooping-learned entries in the Layer 2 table.

The information that is displayed in the show mac-address-table unicast-flood command output is as follows:

- Up to 50 flood entries, shared across all the VLANs that are not configured to use the filter mode, can be recorded.
- The output field displays are defined as follows:
  - ALERT--Information is updated approximately every 3 seconds.
  - SHUTDOWN--Information is updated approximately every 3 seconds.

Note The information displayed on the destination MAC addresses is deleted as soon as the floods stop after the port shuts down.

- Information is updated each time that you install the filter. The information lasts until you remove the filter.

The dynamic entries that are displayed in the Learn field are always set to Yes.

The **show mac-address-table limit** command output displays the following information:

- The current number of MAC addresses.
- The maximum number of MAC entries that are allowed.
- The percentage of usage.

The show mac-address-table synchronize statistics command output displays the following information:

- Number of messages processed at each time interval.
- Number of active entries sent for synchronization.
- Number of entries updated, created, ignored, or failed.

Examples

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

```
Switch# show mac-address-table

Dynamic Addresses Count:              9
Secure Addresses (User-defined) Count: 0
```

```
Static Addresses (User-defined) Count: 0
System Self Addresses Count:           41
Total MAC addresses:                   50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic          1  FastEthernet0/1
0010.7b00.1540       Dynamic          2  FastEthernet0/5
0010.7b00.1545       Dynamic          2  FastEthernet0/5
0060.5cf4.0076       Dynamic          1  FastEthernet0/1
0060.5cf4.0077       Dynamic          1  FastEthernet0/1
0060.5cf4.1315       Dynamic          1  FastEthernet0/1
0060.70cb.f301       Dynamic          1  FastEthernet0/1
00e0.1e42.9978       Dynamic          1  FastEthernet0/1
00e0.1e9f.3900       Dynamic          1  FastEthernet0/1
```

Examples

The following example shows how to display the MAC address table entries that have a specific protocol type (in this case, “assigned”):

```
Switch# show mac-address-table protocol assigned

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0050.3e8d.6400  static   assigned  --  Switch
 100  0050.3e8d.6400  static   assigned  --  Switch
   5  0050.3e8d.6400  static   assigned  --  Switch
4092  0000.0000.0000  dynamic  assigned  --  Switch
   1  0050.3e8d.6400  static   assigned  --  Switch
   4  0050.3e8d.6400  static   assigned  --  Switch
4092  0050.f0ac.3058  static   assigned  --  Switch
4092  0050.f0ac.3059  dynamic  assigned  --  Switch
   1  0010.7b3b.0978  dynamic  assigned  --  Fa5/9
```

The following example shows the “other” output for the previous example:

```
Switch# show mac-address-table protocol other

Unicast Entries
 vlan   mac address     type        protocols               port
-------+---------------+--------+---------------------+--------------------
   1    0000.0000.0201   dynamic other                 FastEthernet6/15
   1    0000.0000.0202   dynamic other                 FastEthernet6/15
   1    0000.0000.0203   dynamic other                 FastEthernet6/15
   1    0000.0000.0204   dynamic other                 FastEthernet6/15
   1    0030.94fc.0dff    static ip,ipx,assigned,other  Switch
   2    0000.0000.0101   dynamic other                 FastEthernet6/16
   2    0000.0000.0102   dynamic other                 FastEthernet6/16
   2    0000.0000.0103   dynamic other                 FastEthernet6/16
   2    0000.0000.0104   dynamic other                 FastEthernet6/16
Fa6/1   0030.94fc.0dff    static ip,ipx,assigned,other  Switch
Fa6/2   0030.94fc.0dff    static ip,ipx,assigned,other  Switch
Multicast Entries
 vlan    mac address     type    ports
-------+---------------+-------+-----------------------------------------
   1    ffff.ffff.ffff   system Switch,Fa6/15
   2    ffff.ffff.ffff   system Fa6/16
1002    ffff.ffff.ffff   system
1003    ffff.ffff.ffff   system
1004    ffff.ffff.ffff   system
1005    ffff.ffff.ffff   system
Fa6/1   ffff.ffff.ffff   system Switch,Fa6/1
Fa6/2   ffff.ffff.ffff   system Switch,Fa6/2
```

Examples

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

```
Switch# show mac-address-table

Dynamic Addresses Count:                 9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:             41
Total MAC addresses:                     50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic          1  FastEthernet0/1
0010.7b00.1540       Dynamic          2  FastEthernet0/5
0010.7b00.1545       Dynamic          2  FastEthernet0/5
0060.5cf4.0076       Dynamic          1  FastEthernet0/1
0060.5cf4.0077       Dynamic          1  FastEthernet0/1
0060.5cf4.1315       Dynamic          1  FastEthernet0/1
0060.70cb.f301       Dynamic          1  FastEthernet0/1
00e0.1e42.9978       Dynamic          1  FastEthernet0/1
00e0.1e9f.3900       Dynamic          1  FastEthernet0/1
```

Note In a distributed Encoded Address Recognition Logic (EARL) switch, the asterisk (*) indicates a MAC address that is learned on a port that is associated with this EARL.

The following example shows how to display the information about the MAC address table for a specific MAC address with a Supervisor Engine 720:

```
Switch# show mac-address-table address 001.6441.60ca

Codes: * - primary entry
  vlan   mac address     type    learn qos            ports
------+---------------+--------+-----+---+--------------------------
Supervisor:
*  ---  0001.6441.60ca    static  No    --  Router
```

The following example shows how to display MAC address table information for a specific MAC address with a Supervisor Engine 720:

```
Router# show mac-address-table address 0100.5e00.0128

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available
  vlan   mac address     type    learn     age              ports
------+---------------+--------+-----+----------+--------------------------
Supervisor:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
Module 9:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
```

The following example shows how to display the currently configured aging time for all VLANs:

```
Switch# show mac-address-table aging-time

Vlan    Aging Time
----    ----------
*100     300
200     1000
```

The following example shows how to display the entry count for a specific slot:

```
Switch# show mac-address-table count module 1

MAC Entries on slot 1 :
Dynamic Address Count:                 4
Static Address (User-defined) Count:  25
Total MAC Addresses In Use:           29
Total MAC Addresses Available:        131072
```

The following example shows how to display the information about the MAC address table for a specific interface with a Supervisor Engine 720:

```
Switch# show mac-address-table interface fastethernet 6/45

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available
  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
*   45  00e0.f74c.842d   dynamic  Yes          5   Fa6/45
```

Note A leading asterisk (*) indicates entries from a MAC address that was learned from a packet coming from an outside device to a specific module.

The following example shows how to display the limit information for a specific slot:

```
Switch# show mac-address-table limit vlan 1 module 1

vlan    switch   module    action      maximum  Total entries  flooding
-------+--------+---------+-----------+--------+--------------+------------
1          1        7       warning      500      0             enabled
1          1        11      warning      500      0             enabled
1          1        12      warning      500      0             enabled

Router#show mac-address-table limit vlan 1 module 2

vlan    switch   module    action      maximum  Total entries  flooding
-------+--------+---------+-----------+--------+--------------+------------
1          2         7      warning      500      0             enabled
1          2         9      warning      500      0             enabled
```

The following example shows how to display the MAC-move notification status:

```
Switch# show mac-address-table notification mac-move

MAC Move Notification: Enabled
```

The following example shows how to display the MAC move statistics:

```
Router# show mac-address-table notification mac-move counter

-------------------------------------------------------------------------------------
Vlan Mac Address From Mod/Port To Mod/Port Count
---- ----------------- ---------------------- ---------------------- ------------
1 00-01-02-03-04-01 2/3 3/1 10
20 00-01-05-03-02-01 5/3 5/1 20
```

The following example shows how to display the CAM-table utilization-notification status:

```
Router# show mac-address-table notification threshold
```

```
Status limit Interval
-------------+-----------+-------------
enabled 1 120
```

The following example shows how to display the MAC notification parameters and history table:

```
Switch# show mac-address-table notification change

MAC Notification Feature is Disabled on the switch
MAC Notification Flags For All Ethernet Interfaces :
----------------------------------------------------
Interface                   MAC Added Trap MAC Removed Trap
--------------------        -------------- ----------------
```

The following example shows how to display the MAC notification parameters and history table for a specific interface:

```
Switch# show mac-address-table notification change interface gigabitethernet5/2

MAC Notification Feature is Disabled on the switch
Interface                   MAC Added Trap MAC Removed Trap
--------------------        -------------- ----------------
GigabitEthernet5/2          Disabled       Disabled
```

The following example shows how to display unicast-flood information:

```
Switch# show mac-address-table unicast-flood

> > Unicast Flood Protection status: enabled
> >
> > Configuration:
> > vlan Kfps action timeout
> > ------+----------+-----------------+----------
> > 2 2 alert none
> >
> > Mac filters:
> > No. vlan source mac addr. installed
> > on time left (mm:ss)
> >
> >-----+------+-----------------+------------------------------+------------------
> >
> > Flood details:
> > Vlan source mac addr. destination mac addr.
> >
> >------+---------------+-------------------------------------------------
> > 2 0000.0000.cafe 0000.0000.bad0, 0000.0000.babe,
> > 0000.0000.bac0
> > 0000.0000.bac2, 0000.0000.bac4,
> > 0000.0000.bac6
> > 0000.0000.bac8
> > 2 0000.0000.caff 0000.0000.bad1, 0000.0000.babf,
> > 0000.0000.bac1
> > 0000.0000.bac3, 0000.0000.bac5,
> > 0000.0000.bac7
> > 0000.0000.bac9
```

The following example shows how to display the information about the MAC-address table for a specific VLAN:

```
Switch#show mac-address-table vlan 100

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 100  0050.3e8d.6400  static   assigned  --  Router
 100  0050.7312.0cff  dynamic        ip  --  Fa5/9
 100  0080.1c93.8040  dynamic        ip  --  Fa5/9
 100  0050.3e8d.6400  static        ipx  --  Router
 100  0050.3e8d.6400  static      other  --  Router
```

```
 100  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 100  00d0.5870.a4ff  dynamic        ip  --  Fa5/9
 100  00e0.4fac.b400  dynamic        ip  --  Fa5/9
 100  0100.5e00.0001  static         ip  --  Fa5/9,Switch
 100  0050.3e8d.6400  static         ip  --  Router
```

The following example shows how to display the information about the MAC address table for MLDv2 snooping:

```
Switch# show mac-address-table multicast mld-snooping

vlan mac address type learn qos ports
-----+---------------+--------+-----+---+--------------------------------
--- 3333.0000.0001 static Yes - Switch,Stby-Switch
--- 3333.0000.000d static Yes - Fa2/1,Fa4/1,Router,Switch
--- 3333.0000.0016 static Yes - Switch,Stby-Switch
```

The table below describes the significant fields shown in the displays.

Table 52: show mac-address-table Field Descriptions

Field	Description
Dynamic Addresses Count	Total number of dynamic addresses in the MAC address table.
Secure Addresses (User-defined) Count	Total number of secure addresses in the MAC address table.
Static Addresses (User-defined) Count	Total number of static addresses in the MAC address table.
System Self Addresses Count	Total number of addresses in the MAC address table.
Total MAC addresses	Total MAC addresses in the MAC address table.
Destination Address	Destination addresses present in the MAC address table.
Address Type	Address type: static or dynamic.
VLAN	VLAN number.
Destination Port	Destination port information present in the MAC address table.
mac address	The MAC address of the entry.
protocol	Protocol present in the MAC address table.
qos	Quality of service associated with the MAC address table.
ports	Port type.

Field	Description
age	The time in seconds since last occurrence of the interface.
Aging Time	Aging time for entries.
module	Module number.
action	Type of action.
flooding	Status of the flooding.

Related Commands

Command	Description
clear mac-address-table	Deletes entries from the MAC address table.
mac-address-table aging-time	Configures the aging time for entries in the Layer 2 table.
mac-address-table limit	Enables MAC limiting.
mac-address-table notification mac-move	Enables MAC-move notification.
mac-address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.
mac-address-table synchronize	Synchronizes the Layer 2 MAC address table entries across the PFC and all the DFCs.
show mac-address-table static	Displays only static MAC address table entries.

show management-interface

To display information about management interfaces, use the **show management-interface** command in privileged EXEC mode.

show management-interface [*interface*| **protocol** *protocol-name*]

Syntax Description

interface	(Optional) Interface for which you want to view information.
protocol	(Optional) Indicates that a protocol is specified.
protocol-name	(Optional) Protocol for which you want to view information.

Command Default

Information about all dedicated management interfaces is displayed when no interface or protocol is specified.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **show management-interface** command allows you to view all management interface configurations and activity on a device and to filter the output by interface or protocol. This flexibility is useful for network monitoring and troubleshooting.

Examples

The following sample output is from a **show management-interface** command when no interface or protocol is specified:

```
Router# show management-interface
Management interface FastEthernet0/0
        Protocol        Packets processed
             ssh                223981
```

The following sample output is from a **show management-interface**commandwith interfaceFastEthernet 0/0specified:

```
Router# show management-interface fastEthernet 0/0
Management interface FastEthernet0/0
        Protocol        Packets processed
             ssh                223981
```

The following sample output is from a **show management-interface**command with protocol Secure Shell (SSH) specified:

```
Router# show management-interface protocol ssh
The following management-interfaces allow protocol ssh
        FastEthernet0/0 Packets processed 223981
```

The table below describes the significant fields shown in the displays.

Table 53: show management-interface Field Descriptions

Field	Description
Management interface <interface>	Interface designated as a management interface.
Protocol	Network management protocols enabled on the interface.
Packets processed	The number of packets processed on the interface.

Related Commands

Command	Description
management-interface allow	Configures an interface to accept only network management packets.

show mls acl inconsistency

To display results from the Multi-Link Switching (MLS) Ternary Content Addressable Memory (TCAM) access check list (ACL) consistency checker, use the **show mls acl inconsistency** command in user EXEC or privileged EXEC mode.

show mls acl inconsistency [**log**| **now**] [**module** *module-number*]

Syntax Description

log	(Optional) Displays contents of the inconsistency log.
now	(Optional) Runs the consistency checker and displays results.
module *module-number*	(Optional) Restricts output to information about the specified module in your device. The value is 1 to 6.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.3(1)S	This command was introduced.

Usage Guidelines

Use this command to verify that the consistency checker is enabled and display the results of the consistency check. The output of this command is self explanatory.

Use this command with the **run** keyword to run a consistency check immediately after the command is issued and to displays the results.

Use this command with the **module** *module-number* keyword and argument combination to display inconsistencies for a specific module in your device.

Examples

```
Device# show mls acl inconsistency

Consistency Check                    : ON
Diagnostics Running                  : NO
Consistency Check Interval(seconds)  : 180
Consistency Check Count              : 4
Last Consistency Check At            : Oct 16 08:48:57.987
TCAM Entry Consistency Check Errors  : 0
TCAM Mask Consistency Check Errors   : 0
Result SRAM Consistency Check Errors : 0
Device# show mls acl inconsistency log

Consistency Check                    : ON
Diagnostics Running                  : NO
```

```
Consistency Check Interval(seconds)  : 180
Consistency Check Count              : 459
Last Consistency Check At            : Oct 17 07:32:30.874
TCAM Entry Consistency Check Errors  : 0
TCAM Mask Consistency Check Errors   : 0
Result SRAM Consistency Check Errors : 0
Device# show mls acl inconsistency now

Running consistency checker now ...
Finished consistency checking
TCAM Entry Consistency Check Errors        : 0
TCAM Mask Consistency Check Errors         : 0
Result SRAM Consistency Check Errors       : 0
Device# show mls acl inconsistency module 1
No forwarding engine in module 1
```

Related Commands

Command	Description
mls acl tcam consistency enable	Enables the MLS ACL TCAM consistency checker.

show mls rate-limit

To display information about the MLS rate limiter in the EXEC command mode, use the **show mls rate-limit** command.

show mls rate-limit [usage]

Syntax Description

usage	(Optional) Displays the feature that is used with the rate-limiter register.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The command output was changed to include hardware rate-limiting status.
12.2(17b)SXA	The command output was changed to display a hyphen (-) instead of an asterisk (*) to indicate that the multicast partial-SC rate limiter is disabled.
12.2(18)SXD	The command output was changed to display IPv6 information.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

In the command output, the rate-limit status could be one of the following:

- On indicates a rate for that particular case has been set.
- Off indicates that the rate-limiter type has not been configured, and the packets for that case are not rate limited.
- On/Sharing indicates a partic ular case (not manually configured) is affected by the configuration of another rate limiter belonging to the same sharing group.
- A hyphen indicates that the multicast partial-SC rate limiter is disabled.

In the command output, the rate-limit sharing indicates the following information:

- Whether sharing is static or dynamic

- Group dynamic sharing codes

The **show mls rate-limit usage** command displays the hardware register that is used by a rate-limiter type. If the register is not used by any rate-limiter type, Free is displayed in the output. If the register is used by a rate-limiter type, Used and the rate-limiter type are displayed.

Examples

This example shows how to display information about the rate-limit status:

```
Router# show mls rate-limit
Sharing Codes: S - static, D - dynamic
 Codes dynamic sharing: H - owner (head) of the group, g - guest of the group
   Rate Limiter Type       Status     Packets/s   Burst  Sharing
 ---------------------   ----------   ---------   -----  -------
         MCAST NON RPF   Off                  -       -     -
        MCAST DFLT ADJ   On              100000     100  Not sharing
      MCAST DIRECT CON   Off                  -       -     -
        ACL BRIDGED IN   Off                  -       -     -
       ACL BRIDGED OUT   Off                  -       -     -
           IP FEATURES   Off                  -       -     -
          ACL VACL LOG   On                2000       1  Not sharing
            MAC PBF IN   Off                  -       -     -
           CEF RECEIVE   Off                  -       -     -
             CEF GLEAN   Off                  -       -     -
      MCAST PARTIAL SC   On              100000     100  Not sharing
        IP RPF FAILURE   On                 100      10  Group:0 S
           TTL FAILURE   Off                  -       -     -
 ICMP UNREAC. NO-ROUTE   On                 100      10  Group:0 S
 ICMP UNREAC. ACL-DROP   On                 100      10  Group:0 S
         ICMP REDIRECT   Off                  -       -     -
           MTU FAILURE   Off                  -       -     -
       MCAST IP OPTION   Off                  -       -     -
       UCAST IP OPTION   Off                  -       -     -
           LAYER_2 PDU   Off                  -       -     -
            LAYER_2 PT   Off                  -       -     -
      LAYER_2 PORTSEC    Off                  -       -     -
    LAYER_2 MiniProto    Off                  -       -     -
     DHCP Snooping IN    Off                  -       -     -
    DHCP Snooping OUT    Off                  -       -     -
       ARP Inspection    Off                  -       -     -
            IP ERRORS    On                 100      10  Group:0 S
          CAPTURE PKT    Off                  -       -     -
           MCAST IGMP    Off                  -       -     -
 MCAST IPv6 DIRECT CON   Off                  -       -     -
 MCAST IPv6 ROUTE CNTL   Off                  -       -     -
 MCAST IPv6 *G M BRIDG   Off                  -       -     -
  MCAST IPv6 SG BRIDGE   Off                  -       -     -
  MCAST IPv6 DFLT DROP   Off                  -       -     -
 MCAST IPv6 SECOND. DR   Off                  -       -     -
  MCAST IPv6 *G BRIDGE   Off                  -       -     -
        MCAST IPv6 MLD   Off                  -       -     -
  IP ADMIS. ON L2 PORT   Off                  -       -     -
        MCAST IPv4 PIM   Off                  -       -     -
Router#
```

This example shows how to display information about the rate-limit usage:

```
Router # show mls rate-limit usage
Rate Limiter Type     Packets/s   Burst
                     ----------------------   ---------   -----
Layer3 Rate Limiters:
             RL# 0: Free                          -           -       -
             RL# 1: Free                          -           -       -
             RL# 2: Free                          -           -       -
             RL# 3: Free                          -           -       -
             RL# 4: Free                          -           -       -
             RL# 5: Used
                                  IP RPF FAILURE         100      10
                                ICMP UNREAC. NO-ROUTE    100      10
```

```
                            ICMP UNREAC. ACL-DROP         100      10
                                       IP ERRORS          100      10
             RL# 6: Used
                                    ACL VACL LOG         2000       1
             RL# 7: Used
                                  MCAST DFLT ADJ       100000     100
             RL# 8: Rsvd for capture                -          -       -
Layer2 Rate Limiters:
             RL# 9: Reserved
             RL#10: Reserved
                                MCAST PARTIAL SC       100000     100
             RL#11: Free                            -          -       -
             RL#12: Free                            -          -       -
Router #
```

Related Commands

Command	Description
mls rate-limit multicast ipv4	Enables and sets the rate limiters for the IPv4 multicast packets.
mls rate-limit multicast ipv6	Configures the IPv6 multicast rate limiters.
mls rate-limit unicast acl	Enables and sets the ACL-bridged rate limiters.

show monitor event-trace dmvpn

To display Dynamic Multipoint VPN (DMVPN) trace information, use the **show monitor event-trace dmvpn** command in privileged EXEC mode.

show monitor event-trace dmvpn [**merged**| **nhrp** {**event**| **error**| **exception**}| **tunnel [parameters]**] {**all**| **back** *time*| **clock** *hh* **:** *mm* [*day month*| *month day*]| **from-boot** [*boot-time*]| **latest**} **[detail]**

Syntax Description

merged	(Optional) Displays all traces in the current buffer.
nhrp	(Optional) Displays Next Hop Resolution Protocol (NHRP) traces.
event	(Optional) Displays NHRP event traces.
error	(Optional) Displays NHRP error traces.
exception	(Optional) Displays NHRP exception traces.
tunnel	(Optional) Displays tunnel events.
parameters	(Optional) Displays parameters of the trace.
all	Displays all traces in the current buffer.
back *time*	Displays traces since the specified time. Time can be specified as minutes (*mmm*) or in hour:minute (*hh* **:** *mm*) format.
clock *hh* **:** *mm*	Displays trace from the specified time.
day	(Optional) Day in a month.
month	(Optional) Month of a year.
from-boot	Displays trace after the specified time after boot.
boot-time	(Optional) Time specified to wait to display trace after boot.
latest	Displays the latest trace events since the previous display.
detail	(Optional) Displays detailed trace information.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines You can use the **show monitor event-trace dmvpn** command to verify DMVPN event tracing.

This command displays all the tunnel events, including the DMVPN tunnel events and the non-DMVPN tunnel events.

Note The **show monitor event-trace dmvpn** command output displays all tunnel events. You dare not able to filter only the DMVPN tunnel information in the display.

Examples The following is sample output from the **show monitor event -trace dmvpn nhrp exception all** command. The fields in the display are self-explanatory.

```
Router# show monitor event-trace dmvpn nhrp exception all

ev_type : NHS-UP trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHS-UP  Tunnel0 : NHS UP,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1
ev_type : NHS-DOWN trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHS-DOWN  Tunnel0 : NHS DOWN,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1, reason: External
ev_type : NHC-UP trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHC-UP  Tunnel0 : NHC UP,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1
ev_type : NHC-DOWN trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHC-DOWN  Tunnel0 : NHC DOWN,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1, reason: External
ev_type : NHP-UP trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHP-UP  Tunnel0 : NHP UP,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1
ev_type : NHP-DOWN trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHP-DOWN  Tunnel0 : NHP DOWN,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1, reason: External
ev_type : NHRP-RATE_LIMIT trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHRP-RATE_LIMIT  Tunnel0 : Max-send Quota of
10000pkts/500sec exceeded
ev_type : NHS-RECOVERY-NHS-STATE trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHS-RECOVERY-NHS-STATE  NHS recovery event string
```

Related Commands

Command	Description
monitor event-trace dmvpn	Monitors and controls DMVPN traces.

show monitor event-trace gdoi

To display information about Group Domain of Interpretation (GDOI) event traces, use the **show monitor event-trace gdoi** command in privileged EXEC mode.

show monitor event-trace gdoi [merged] {**all**| **back** *trace-duration*| **clock** *time* [*day month*]| **from-boot** [*seconds*]| **latest**} **[detail]**

Syntax Description

merged	(Optional) Displays entries in all event traces sorted by time.
all	(Optional) Displays all traces in the current buffer.
back	(Optional) Displays trace over a specified duration from the present to the past.
trace-duration	(Optional) Duration of trace (in minutes or in hours:minutes format). The range is 0 to 4,294,967,295 minutes (or 0 hours and 0 minutes to 4,294,967,295 hours and 59 minutes when specifying hours and minutes).
clock	(Optional) Displays trace from a specific time and date.
time	(Optional) Time from which to show trace (in hours:minutes format).
day	(Optional) Day of the month. The range is 1 to 31.
month	(Optional) Month of the year. Eligible values are January, February, March, April, May, June, July, August, September, October, November, and December.
from-boot	(Optional) Displays trace from a specific number of seconds after booting.
seconds	(Optional) Time after boot in seconds. The range is 0 to 932221.
latest	(Optional) Displays latest trace events since the last display.
detail	(Optional) Displays detailed trace information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Examples

The following is sample stack traces from the **show monitor event-trace gdoi rekey** command.

```
Device# show monitor event-trace gdoi rekey

Event[1] Oct 19 18:02:03.055: %GDOI-5-GM_RECV_REKEY: Received Rekey for group gdoigroup1
from 5.5.90.1 to 228.10.10.10 with seq # 2
 -Traceback= 0x36D90 0xDECBC 0x3CC53 0xFC2C320 0xDFC245
r100#sh monitor event-trace gdoi exit
Event[1] Oct 19 18:02:03.055: Coop Peer not reachable, Peer marked dead.
 -Traceback= 0x3CB04 0xFD2C49 0xFD2C493C
 Event[2] Oct 19 18:02:03.055:  No IKE SA found to peer
 local 16.0.0.1/0 remote 16.0.0.2/500 fvrf 0x0 ivrf 0x0 for SPI 0x120DCC0
 -Traceback= 0x35E90 0xC0CBC 0x3BB54 0xFD2C49 0xFD2C493C
```

Related Commands

Command	Description
monitor event-trace gdoi	Configures event tracing for the GDOI software subsystem component.
monitor event-trace gdoi (privileged EXEC)	Configures event tracing for the GDOI software subsystem component.

show object-group

To display information about configured network or service object groups used in object group access control lists (OGACLs) or user object group information, containing security group or nested group object information, for the class map in a Cisco TrustSec (CTS) Security Group Access (SGA) Zone-Based Policy firewall (ZBPF), use the **show object-group** command in user EXEC or privileged EXEC mode.

show object-group [*object-group-name*]

Syntax Description

name	(Optional) Name of the object group, security group, or group object for which information will be displayed.

Command Default

Information is displayed for all object groups.

Command Modes

Privileged EXEC (#) User EXEC (>)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.2(1)S	This command was introduced in Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.5	This command was introduced in Cisco IOS XE Release 3.5.

Examples

The following example displays **show object-group** command output of network and service object groups in an OGACL configuration:

```
Router# show object-group
Network object group auth_proxy_acl_deny_dest
 host 171.68.225.134
Service object group auth_proxy_acl_deny_services
 tcp eq www
 tcp eq 443
Network object group auth_proxy_acl_permit_dest
 10.34.250.96 255.255.255.224
 171.68.0.0 255.252.0.0
 172.16.0.0 255.240.0.0
 128.107.0.0 255.255.0.0
 10.0.0.0 255.0.0.0
 64.100.0.0 255.253.0.0
 64.104.0.0 255.255.0.0
 144.254.0.0 255.255.0.0
 161.44.0.0 255.255.0.0
 192.168.0.0 255.255.0.0
Service object group auth_proxy_acl_permit_services
```

```
 tcp eq www
 tcp eq 443
```

The table below describes the significant fields shown in the command output.

Table 54: show object-group Field Descriptions (OGACL Configuration)

Field	Description
Network object group auth_proxy_acl_deny_dest	Name of the network object group.
host 171.68.225.134	IP address of the host object.
Network object group auth_proxy_acl_deny_services	Name of the service object group.
tcp eq www tcp eq 443	TCP port types.
10.34.250.96 255.255.255.224	Network address and network mask of the subnet object.

The following example displays **show object-group** command output that shows user object group information for the class map in a CTS SGA ZBPF configuration:

```
Router# show object-group

User object group objsgt1
 security-group 120

User object group objsgt2
 group-object objsgt1
```

The table below describes the significant fields shown in the command output.

Table 55: show object-group Field Descriptions (CTS SGA ZBPF Configuration)

Field	Description
User object group	Name of the object group used to identify traffic coming from a specific user or endpoint in the CTS SGA ZBPF.
security-group	The securtiy group, identified by its Security Group Tag (SGT) identification number, that belongs to a user object group in the CTS SGA ZBPF.
group-object	The nested reference to a type of user group within an object group in the CTS SGA ZBPF.

Related Commands

Command	Description
debug object-group event	Enables debug messages for object-group events.

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
group-object	Specifies a nested reference to a type of user group.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
match group-object security	Matches traffic from a user in the security group.
object-group network	Defines network object groups for use in OGACLs.
object-group security	Creates an object group to identify traffic coming from a specific user or endpoint.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
security-group	Specifies the membership of the security group for an object group.
show ip access-list	Displays the contents of IP access lists or OGACLs.