show diameter peer through show object-group

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 1: 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 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 2: 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 3: 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 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.

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 4: 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.
Inbound access list	Shows whether the interface has an incoming access list set.

Field	Description
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.
IP output packet accounting	Shows whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.

Field	Description
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 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
```

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

Table 5: show ip interface brief Field Descriptions

Field	Description
Interface	Type of interface.
IP-Address	IP address assigned to the interface.
OK?	"Yes" means that the IP Address is valid. "No" means that the IP Address is not valid.

Field	Description
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 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 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 6: 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 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 7: 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-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 8: 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.