mac access-group through private-vlan mapping

mac access-group

To use a MAC access control list (ACL) to control the reception of incoming traffic on a Gigabit Ethernet interface, an 802.1Q VLAN subinterface, an 802.1Q-in-Q stacked VLAN subinterface, use the **macaccess-group**command in interface or subinterface configuration mode. To remove a MAC ACL, use the **no** form of this command.

mac access-group *access-list-number* **in**

no mac access-group *access-list-number* **in**

Syntax Description

access-list-number	Number of a MAC ACL to apply to an interface or subinterface (as specified by a **access-list(MAC)** command). This is a decimal number from 700 to 799.
in	Filters on inbound packets.

Command Default

No access list is applied to the interface or subinterface.

Command Modes

Interface configuration (config-if) Subinterface configuration (config-subif)

Command History

Release	Modification
12.0(32)S	This command was introduced on the Cisco 12000 series Internet router.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

MAC ACLs are applied on incoming traffic on Gigabit Ethernet interfaces and VLAN subinterfaces. After a networking device receives a packet, the Cisco IOS software checks the source MAC address of the Gigabit Ethernet, 802.1Q VLAN, or 802.1Q-in-Q packet against the access list. If the MAC access list permits the address, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns an Internet Control Message Protocol (ICMP) host unreachable message.

If the specified MAC ACL does not exist on the interface or subinterface, all packets are passed.

On Catalyst 6500 series switches, this command is supported on Layer 2 ports only.

Note The **macaccess-group**command is supported on a VLAN subinterface only if a VLAN is already configured on the subinterface.

Examples

The following example applies MAC ACL 101 on incoming traffic received on Gigabit Ethernet interface 0:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# mac access-group 101 in
```

Related Commands

Command	Description
access-list (MAC)	Defines a MAC ACL.
clear mac access-list counters	Clears the counters of a MAC ACL.
ip access-group	Configures an IP access list to be used for packets transmitted from the asynchronous host.
show access-group mode interface	Displays the ACL configuration on a Layer 2 interface.
show mac access-list	Displays the contents of one or all MAC ACLs.

mac access-list extended

To create an extended MAC access control list (ACL) and define its access control entries (ACEs), use the **macaccess-listextended** command in global configuration mode. To remove MAC ACLs, use the **no** form of this command.

mac access-list extended *name*

no mac access-list extended *name*

Syntax Description

name	Name of the ACL to which the entry belongs.

Command Default

No extended ACLs are defined.

Command Modes

Global configuration (config)

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 as follows: • Add the **vlan***vlan* and **cos***value* keywords and arguments. • Add the **ip** keyword to the list of valid protocol names.
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 12.2(33)SRA.
12.2(33)SRD	The following Ethertype protocol values were added to the valid protocol list: **bpdu-sap**, **bpdu-snap**, **dtp**, **lacp**, **pagp**, **vtp**.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on Cisco ASR 901Series Aggregation Service Routers.

When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)

- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are **all**, **default-action**, **map**, **help**, and **editbuffer**

You can configure named ACLs that filter Internet Packet Exchange (IPX), DECnet, AppleTalk, Virtual Integrated Network Service (VINES), or Xerox Network Services (XNS) traffic based on MAC addresses (IPX filtering with a MAC ACL is supported only with a Policy Feature Card 3 [PFC3]).

In systems that are configured with PFC3, if you want to classify all IPX traffic by using a MAC-access list that matches on EtherType 0x8137, use the **ipx-arpa** or **ipx-non-arpa** protocol.

Once you enter the **macaccess-listextended***name* command, use the following subset to create or delete entries in a MAC ACL:

no permit deny *src-mac mask* **any** *dest-mac mask* **any** *protocol* **vlan** *vlan* **cos** *value*

The **vlan***vlan* and **cos***value* keywords and arguments are supported in PFC3BXL or PFC3B mode with Release 12.2(17b)SXA and later releases.

The **vlan***vlan* and **cos***value* keywords and arguments are not supported on the MAC VLAN access control lists (VACLs).

The table below describes the syntax of the **macaccess-listextended** command.

Table 1: mac access-list extended Command Syntax

Syntax	Description
no	(Optional) Deletes a statement from an access list.
permit	Permits access if the conditions are matched.
deny	Denies access if the conditions are matched.
src-mac mask	Source MAC address in the form: *source-mac-addresssource-mac-address-mask*.
any	Specifies any protocol type.
dest-mac mask	(Optional) Destination MAC address in the form: *dest-mac-addressdest-mac-address-mask*.
protocol	(Optional) Name or number of the protocol; see below for a list of valid entries for this argument.
vlan vlan	(Optional) Specifies a VLAN ID; valid values are from 0 to 4095.

Syntax	Description
cos value	(Optional) Specifies a CoS value; valid values are from 0 to 7.

Valid entries for the *protocol* argument are as follows:

- **0x0-0xFFFF** --Arbitrary EtherType in hexadecimal
- **aarp** --EtherType: AppleTalk Address Resolution Protocol (ARP)
- **amber** --EtherType: DEC-Amber
- **appletalk** --EtherType: AppleTalk/EtherTalk
- **bpdu-sap** --BPDU SAP encapsulated packets
- **bpdu-snap** --BPDU SNAP encapsulated packets
- **dec-spanning** --EtherType: DEC-Spanning-Tree
- **decnet-iv** --EtherType: DECnet Phase IV
- **diagnostic** --EtherType: DEC-Diagnostic
- **dsm** --EtherType: DEC-DSM
- **dtp** --DTP packets
- **etype-6000** --EtherType: 0x6000
- **etype-8042** --EtherType: 0x8042
- **ip** --EtherType: 0x0800
- **ipx-arpa** --IPX Advanced Research Projects Agency (ARPA)
- **ipx-non-arpa** --IPX non-ARPA
- **lacp** --**LACPencapsulatedpackets**
- **lat** --EtherType: DEC-LAT
- **lavc-sca** --EtherType: DEC-LAVC-SCA
- **mop-console** --EtherType: DEC-MOP Remote Console
- **mop-dump** --EtherType: DEC-MOP Dump
- **msdos** --EtherType: DEC-MSDOS
- **mumps** --EtherType: DEC-MUMPS
- **netbios** --EtherType: DEC-NETBIOS
- **pagp** --PAGP encapsulated packets
- **vines-echo** --EtherType: VINES Echo
- **vines-ip** --EtherType: VINES IP
- **vtp** --VTP packets

- **xns-idp** --EtherType: XNS IDP

When you enter the *src-macmask* or *dest-macmask*value, note these guidelines and restrictions:

- Enter MAC addresses as three 4-byte values in dotted hexadecimal format; for example, 0030.9629.9f84.
- Enter MAC-address masks as three 4-byte values in dotted hexadecimal format. Use 1 bit as a wildcard. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- For the optional *protocol*, you can enter either the EtherType or the keyword.
- Entries without a *protocol* match any protocol.
- Access lists entries are scanned in the order that you enter them. The first matching entry is used. To improve performance, place the most commonly used entries near the beginning of the access list.
- An implicit **denyanyany** entry exists at the end of an access list unless you include an explicit **permitanyany** entry at the end of the list.
- All new entries to an existing list are placed at the end of the list. You cannot add entries to the middle of a list.

Malformed, invalid, deliberately corrupt EtherType 0x800 IP frames are not recognized as IP traffic and are not filtered by IP ACLs.

An ACE created with the **macaccess-listextended** command with the **ip** keyword filters malformed, invalid, deliberately corrupt EtherType 0x800 IP frames only; it does not filter any other IP traffic.

Examples

The following example shows how to create a MAC ACL named mac_layer that denies traffic from 0000.4700.0001, which is going to 0000.4700.0009, and permits all other traffic:

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dsm
Router(config-ext-macl)# permit any any
```

Related Commands

Command	Description
mac access-group in	Applies MAC ACLs to Ethernet service instances.
show mac-address-table	Displays information about the MAC address table.

mac-address-table aging-time

To configure the maximum aging time for entries in the Layer 2 table, use the **mac-address-tableaging-time** command in global configuration mode. To reset maximum aging time to the default setting, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

mac-address-table aging-time *seconds*

no mac-address-table aging-time *seconds*

Cisco 7600 Series Routers

mac-address-table aging-time *seconds* [**routed-mac**| **vlan** *vlan-id*]

no mac-address-table aging-time *seconds* [**routed-mac**| **vlan** *vlan-id*]

Catalyst Switches

mac-address-table aging-time *seconds* [**routed-mac**| **vlan** *vlan-id*]

no mac-address-table aging-time *seconds* [**routed-mac**| **vlan** *vlan-id*]

Syntax Description

seconds	MAC address table entry maximum age. Valid values are 0, and from 5 to 1000000 seconds. Aging time is counted from the last time that the switch detected the MAC address. The default value is 300 seconds.
vlan *vlan -id*	(Optional) Specifies the VLAN to which the changed aging time should be applied. Valid values are from 2 to 1001.
routed-mac	(Optional) Specifies the routed MAC aging interval.
vlan *vlan-id*	(Optional) Specifies the VLAN to apply the changed aging time; valid values are from 1 to 4094.

Command Default

The default aging time is 300 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced on Catalyst 6000 series switches.

Release	Modification
12.1(1)E	This command was implemented on Catalyst 6000 series switches.
12.2(2)XT	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600 series, Cisco 3600 series, and Cisco 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 implemented on Catalyst switches and Cisco 7600 Internet routers with a Supervisor Engine 720.
12.2(17d)SXB	This command was implemented on Cisco Catalyst switches and Cisco 7600 Internet routers with a Supervisor Engine 2.
12.2(18)SXE	The **routed-mac** keyword was added. This keyword is supported only on a Supervisor Engine 720 in Cisco 7600 Internet routers and Catalyst 6500 switches.
12.2(18)SXF5	The minimum value for the *seconds* argument was changed from 10 to 5.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	The output for this command was modified to include additional fields and explanatory text.

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The aging time entry will take the specified value. Valid entries are from 10 to 1000000 seconds.

This command cannot be disabled.

Catalyst Switches and Cisco 7600 Routers

If you do not enter a VLAN, the change is applied to all routed-port VLANs.

Enter 0 seconds to disable aging.

You can enter the **routed-mac** keyword to configure the MAC address aging time for traffic that has the routed MAC (RM) bit set.

Examples

Examples

The following example shows how to configure aging time to 300 seconds:

```
mac-address-table aging-time 300
```

Examples

The following example shows how to configure the aging time:

```
mac-address-table aging-time 400
```

The following example shows how to change the RM aging time to 500 seconds:

```
mac-address-table aging-time 500 routed-mac
```

The following example shows how OOB affects modifying the aging-time:

```
mac-address-table aging-time 250
%% Vlan Aging time not changed since OOB is enabled and requires aging time to be atleast
3 times OOB interval - default: 480 seconds
```

The following example shows how to disable the aging time:

```
mac-address-table aging-time 0
```

Related Commands

Command	Description
show mac-address-table	Displays information about the MAC address table.
show mac address table aging time	Displays the MAC address aging time.

mac-address-table dynamic

To add dynamic addresses to the MAC address table, use the **mac-address-tabledynamic**command in global configuration mode. Dynamic addresses are automatically added to the address table and dropped from it when they are not in use. To remove dynamic entries from the MAC address table, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

mac-address-table dynamic *hw-addressinterface* {**fa| gi**}[*slot/port*]**vlan** *vlan-id*

no mac-address-table dynamic *hw-address* **vlan** *vlan-id*

Catalyst Switches

no mac-address-table dynamic *hw-address* [**atm** *slot/port*][**vlan** *vlan-id*]

Syntax Description

hw -address	MAC address added to or removed from the table.
interface	Port to which packets destined for *hw-address* are forwarded.
fa	Specifies FastEthernet.
gi	Specifies GigabitEthernet.
slot	(Optional) The slot (slot 1 or slot 2) to which to add dynamic addresses.
port	(Optional) Port interface number. The ranges are based on type of Ethernet switch network module used: • 0 to 15 for NM-16ESW • 0 to 35 for NM-36ESW • 0 to 1 for GigabitEthernet
atm *slot /port*	(Optional) Add dynamic addresses to the ATM module in slot 1 or 2. The port is always 0 for an ATM interface.

vlan *vlan -id*	Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers The interface and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded. The **vlan** keyword is optional if the port is a static-access or dynamic-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. The **vlan** keyword is required for multi-VLAN and trunk ports. This keyword is required on trunk ports to specify to which VLAN the dynamic address is assigned. The*vlan-id* is the value of the ID of the VLAN to which packets destined for *hw-address* are forwarded. Valid IDs are 1 to 1005; do not enter leading zeroes. Catalyst Switches (Optional) The interface and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded. The **vlan** keyword is optional if the port is a static-access or dynamic-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. **Note** When this command is executed on a dynamic-access port, queries to the VLAN Membership Policy Server (VMPS) do not occur. The VMPS cannot verify that the address is allowed or determine to which VLAN the port should be assigned. This command should be used only for testing purposes. The **vlan** keyword is required for multi-VLAN and trunk ports. This keyword is required on trunk ports to specify to which VLAN the dynamic address is assigned. The*vlan-id* is the value of the ID of the VLAN to which packets destined for *hw-address* are forwarded. Valid IDs are 1 to 1005; do not enter leading zeroes.

Command Default Dynamic addresses are not added to the MAC address table.

Command Modes Global configuration (config)

Command History

Release	Modification
11.2(8)SA	This command was introduced.
11.2(8)SA3	The **vlan** keyword was added.
11.2(8)SA5	The **atm** keyword was added.
12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T, on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
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 your feature set, platform, and platform hardware.

Usage Guidelines

If the *vlan-id* argument is omitted and the **no** form of the command is used, the MAC address is removed from all VLANs.

Examples

The following example shows how to add a MAC address on port fa1/1 to VLAN 4:

```
Switch(config)# mac-address-table dynamic 00c0.00a0.03fa fa1/1 vlan 4
```

Related Commands

Command	Description
clear mac -address-table	Deletes entries from the MAC address table.
mac -address-tableaging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
mac -address-tablestatic	Adds static addresses to the MAC address table.
show mac -address-table	Displays the MAC address table.

mac-address-table limit

To enable the MAC limiting functionality and set the limit to be imposed, use the **mac-address-tablelimit** command in global configuration mode. To disable MAC limiting, use the **no** form of this command.

mac-address-table limit {**action**| }

Syntax Description

maximum *num*	(Optional) Specifies the maximum number of MAC entries per-VLAN per-Encoded Address Recognition Logic (EARL) allowed; valid values are from 5 to 32768 MAC-address entries.
action	(Optional) Specifies the type of action to be taken when the action is violated.
warning	(Optional) Specifies that the one syslog message will be sent and no further action will be taken when the action is violated.
limit	(Optional) Specifies that the one syslog message will be sent and/or a corresponding trap will be generated with the MAC limit when the action is violated.
shutdown	(Optional) Specifies that the one syslog message will be sent and/or the VLAN is moved to the blocked state when the action is violated.
notification	(Optional) Specifies the type of notification to be sent when the action is violated.
syslog	(Optional) Sends a syslog message when the action is violated.
trap	(Optional) Sends trap notifications when the action is violated.
both	(Optional) Sends syslog and trap notifications when the action is violated.
vlan *vlan*	(Optional) Enables MAC limiting on a per-VLAN basis.
interface *type mod* / *port*	(Optional) Enables MAC limiting on a per-port basis.
flood	(Optional) Enables unknown unicast flooding on a VLAN.

Command Default

The defaults are as follows:

- **maximum** *num* is **500** MAC address entries.
- **action** is **warning**
- **notification** is **syslog**

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD1	This command was changed to include the **vlan***vlan* keyword and argument to support per-VLAN MAC limiting.
12.2(18)SXE	This command was changed to include the **interface***typemod/port* keyword and arguments to support per-port MAC limiting.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

MAC limiting can be enabled on either a per-interface basis (that is, by specifying an interface) or on a per-VLAN basis (that is, by specifying a VLAN). However, MAC limiting must first be enabled for the router (a higher level) in global configuration mode (config).

General Points About MAC Limiting

Note the following points about enabling MAC limiting:

- The maximum number of MAC entries is determined on a per-VLAN and per-EARL basis.
- If you do not specify a maximum number, an action, or a notification, the default settings are used.
- If you enable per-VLAN MAC limiting, MAC limiting is enabled on the specified VLAN only.
- The **flood** keyword is supported on VLAN interfaces only.
- The **flood** action occurs only if the **limit** action is configured and is violated.
- In the **shutdown** state, the VLAN remains in the blocked state until you reenable it through the command syntax.

Syntax for Enabling per-VLAN MAC Limiting

The following is sample syntax that can be used to enable per-VLAN MAC limiting. Both commands must be used to properly enable per-VLAN MAC limiting.

mac-address-table limit

Note This command enables the MAC limiting functionality for the router.

mac-address-table limit [**vlan***vlan*] [**maximum***num*] [**action** {**warning** | **limit** | **shutdown**}] [flood]

Note This command sets the specific limit and any optional actions to be imposed at the VLAN level.

Syntax for Enabling Per-Interface MAC Limiting

The following is sample syntax that can be used to enable per-interface MAC limiting. Both commands must be used to properly enable per-interface MAC limiting.

mac-address-table limit

Note This command enables the MAC limiting functionality for the router.

mac-address-table limit [**interface***typemod/port*] [**maximum***num*] [**action** {**warning** | **limit** | **shutdown**}] [flood]

Note This command sets the specific limit and any optional actions to be imposed at the interface level.

Examples

This example shows how to enable per-VLAN MAC limiting. The first instance of the**mac-address-tablelimit** command enables MAC limiting. The second instance of the command sets the limit and any optional actions to be imposed at the VLAN level.

```
Router# enable
Router# configure terminal
Router(config)# mac-address-table limit
Router(config)# mac-address-table limit vlan 501 maximum 50 action shutdown
Router(config)# end
```

This example shows how to enable per-interface MAC limiting. The first instance of the**mac-address-tablelimit** command enables MAC limiting. The second instance of the command sets the limit and any optional actions to be imposed at the interface level.

```
Router# enable
Router# configure terminal
Router(config)# mac-address-table limit
Router(config)# mac-address-table limit fastethernet0/0 maximum 50 action shutdown
Router(config)# end
```

Related Commands

Command	Description
show mac-address-table limit	Displays the information about the MAC-address table.

mac-address-table notification change

To send a notification of the dynamic changes to the MAC address table, use the **mac-address-tablenotificationchange**command in global configuration mode. To return to the default settings, use the **no** form of this command.

mac-address-table notification change [**history** *size*| **interval** *seconds*]

no mac-address-table notification change

Syntax Description

history *size*	(Optional) Sets the number of entries in the history buffer; valid values are from 0 to 500 entries.
interval *seconds*	(Optional) Sets the minimum change sending interval; valid values are from 0 to 2147483647 seconds.

Command Default

The default settings are as follows:

- Disabled
- If notification of the dynamic changes to the MAC address table is enabled, the default settings are as follows:
  - **history***size* is 1 entry.
  - **interval***value* is 1 second.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

This example shows how to configure the Simple Network Management Protocol (SNMP) notification of dynamic additions to the MAC address table of addresses:

```
Router(config)# mac-address-table notification change interval 5 history 25
```

Related Commands

Command	Description
show mac-address-table	Displays information about the MAC address table.

Command	Description
snmp-server trap mac-notification	Enables the SNMP trap notification on a LAN port when MAC addresses are added to or removed from the address table.

mac-address-table notification mac-move

To enable MAC-move notification, use the **mac-address-tablenotificationmac-move** command in global configuration mode. To disable MAC-move notification, use the **no** form of this command.

mac-address-table notification mac-move [**counter [syslog]**]

no mac-address-table notification mac-move [**counter [syslog]**]

Syntax Description

counter	(Optional) Specifies the MAC-move counter feature.
syslog	(Optional) Specifies the syslogging facility when the MAC-move notification detects the first instance of the MAC move .

Command Default

MAC-move notification is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SXI	This command was changed to add the **counter** and the **syslog** keywords.

Usage Guidelines

MAC-move notification generates a syslog message whenever a MAC address or host moves between different switch ports.

MAC-move notification does not generate a notification when a new MAC address is added to the content-addressable memory (CAM) or when a MAC address is removed from the CAM.

MAC-move notification is supported on switch ports only.

The MAC-move counter notification generates a syslog message when the number of MAC moves in a VLAN exceeds the maximum limit. The maximum limit is 1000 MAC moves.

The MAC-move counter syslog notification counts the number of times a MAC has moved within a VLAN and the number of these instances that have occurred in the system.

Examples

This example shows how to enable MAC-move notification:

```
Router(config)# mac-address-table notification mac-move
```

This example shows how to disable MAC-move notification:

```
Router(config)# no mac-address-table notification mac-move
```

This example shows how to enable MAC-move counter syslog notification:

```
Router(config)# mac-address-table notification mac-move counter syslog
```

This example shows how to disable MAC-move counter notification:

```
Router(config)# no mac-address-table notification mac-move counter
```

Related Commands

Command	Description
show mac-address-table notification mac-move	Displays the information about the MAC-address table.
clear mac-address-table notification mac-move	Clears the MAC-address table notification counters.

mac-address-table static

To add static entries to the MAC address table or to disable Internet Group Multicast Protocol (IGMP) snooping for a particular static multicast MAC address, use the **mac-address-table static** command in global configuration mode. To remove entries profiled by the combination of specified entry information, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, Cisco 3700 and Cisco 7600 Series Routers

mac-address-table static *mac-address* **vlan** *vlan-id* **interface** *type slot*/*port*

no mac-address-table static *mac-address* **vlan** *vlan-id* **interface** *type slot*/*port*

Catalyst Switches

mac-address-table static *mac-address* **vlan** *vlan-id* **interface** *type number* **drop** [**disable-snooping**][**dlci** *dlci*| **pvc** *vpi*/*vci*][**auto-learn**| **disable-snooping**][**protocol]** {**ip**| **ipx**| **assigned**}

no mac-address-table static *mac-address* **vlan** *vlan-id***interface** *type number* **drop** [**disable-snooping**][**dlci** *dlci*| **pvc** *vpi*/*vci*][**auto-learn**| **disable-snooping**][**protocol]** {**ip**| **ipx**| **assigned**}

Syntax Description

mac-aadress	Address to add to the MAC address table.
vlan *vlan-id*	Specifies the VLAN associated with the MAC address entry. The range is from 2 to 100.
interface *type slot*/*port* or **interface** *type number*	Specifies the interface type and the slot and port to be configured. On the Catalyst switches, the*type* and *number* arguments should specify the interface type and the *slot*/*port* or *slot*/*subslot*/*port* numbers (for example, **interface pos 5/0** or **interface ATM 8/0/1**).
drop	Drops all traffic that is received from and going to the configured MAC address in the specified VLAN.
disable-snooping	(Optional) Disables IGMP snooping on the multicast MAC address.
dlci *dlci*	(Optional) Specifies the data-link connection identifier (DLCI) to be mapped to this MAC address. Valid values are from 16 to 1007. **Note** This option is available only if Frame Relay encapsulation has been enabled on the specified interface.

pvc *vpi/vci*	(Optional) Specifies the permanent virtual circuit (PVC) to be mapped to this MAC address. You must specify both a virtual path identifier (VPI) and a virtual circuit identifier (VCI), separated by a slash. **Note** This option is available only for ATM interfaces.
auto-learn	(Optional) Specifies that if the router sees this same MAC address on a different port, the MAC entry should be updated with the new port.
disable-snooping	(Optional) Disables IGMP snooping on the Frame Relay DLCI or ATM PVC.
protocol	(Optional) Specifies the protocol associated with the entry.
ip	(Optional) Specifies the IP protocol.
ipx	(Optional) Specifies the Internetwork Packet Exchange (IPX) protocol.
assigned	(Optional) Specifies assigned protocol bucket accounts for protocols such as DECnet, Banyan VINES, and AppleTalk.

Command Default

Static entries are not added to the MAC address table.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced on Catalyst 6000 series switches.
12.1(1)E	Support for this command on Catalyst 6000 series switches was extended to the 12.1E train.
12.1(5c)EX	This command was modified. Support for multicast addresses was added.
12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(17a)SX	You cannot apply the **mac-address-table static** *mac-address* **vlan** *vlan-id* {**interface** *type number* **drop**} command to a multicast MAC address.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXE	This command was modified. The **dlci** *dlci* and **pvc** *vpi*/*vci* keyword-argument pairs were added to allow mapping a MAC address to a Frame Relay DLCI or ATM PVC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. Support was added to High-Speed Serial Interface (HSSI), MLPP, and serial interfaces on Cisco 7600 series routers.

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The specified output interface cannot be a switched virtual interface (SVI).

The**no** form of this command does not remove system MAC addresses.

When you remove a MAC address, entering the **interface** *type slot*/*port* argument is optional. For unicast entries, the entry is removed automatically. For multicast entries, if you do not specify an interface, the entire entry is removed. You can specify the selected ports to be removed by specifying the interface.

Catalyst Switches

The specified output interface cannot be an SVI.

As a good practice, configure static MAC addresses on Layer 2 EtherChannels only and not on Layer 2 physical member ports of an EtherChannel. This practice does not apply to Layer 3 EtherChannels and its members.

Use the **no** form of this command to do the following:

- Remove entries that are profiled by the combination of specified entry information.
- Re-enable IGMP snooping for the specified address.

The **dlci** *dlci* keyword and argument are valid only if Frame Relay encapsulation has been enabled on the specified interface.

The **pvc** *vpi*/*vci* keyword and arguments are supported on ATM interfaces only. When specifying the **pvc***vpi*/*vci* argument and keyword pair, you must specify both a VPI and a VCI, separated by a slash.

When you install a static MAC address, it is associated with a port. If the same MAC address is seen on a different port, the entry is updated with the new port if you enter the **auto-learn** keyword.

The specified output interface must be a Layer 2 Interface Descriptor Block (IDB) and not an SVI.

You can enter up to 15 interfaces per command entered, and you can enter more interfaces by repeating the command.

If you do not enter a protocol type, an entry is automatically created for each of the protocol types.

Entering the **no** form of this command does not remove system MAC addresses.

When you remove a MAC address, entering **interface** *type number* is optional. For unicast entries, the protocol entry is removed automatically. For multicast entries, if you do not specify an interface, the entire protocol entry is removed. You can specify the selected ports to be removed by specifying the interface.

The **mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *type number***disable-snooping** command disables snooping on the specified static MAC address/VLAN pair only. To enable snooping, first delete the MAC address using the **no** form of the command, and then reinstall the MAC address using the **mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *type number* command, without the **disable-snooping** keyword.

The **mac-address-table static** *mac-address* **vlan** *vlan-id* **drop** command cannot be applied to a multicast MAC address.

Note Both the unicast MAC addresses and the multicast MAC addresses allow only one WAN interface.

Note You cannot configure the same static MAC address on multiple interface. If you try to configure an existing static MAC address on another interface, the **mac-address-table static** command overwrites the static MAC address with a new MAC address on this interface.

Specifying a MAC Address for DLCI or PVC Circuits

To support multipoint bridging and other features, the behavior of the following command has changed for ATM and Frame Relay interfaces in Cisco IOS Release 12.2(18)SXE and later releases. In previous releases, you needed to specify a VLAN ID and an interface only.

```
Device(config)# mac-address-table static 000C.0203.0405 vlan 101 interface ATM6/1
```

In Cisco IOS Release 12.2(18)SXE and later releases, you must specify the **dlci** option for Frame Relay interfaces, or the **pvc** option for ATM interfaces, as shown in the following example:

```
Device(config)# mac-address-table static 000C.0203.0405 vlan 101 interface ATM6/1 pvc6/101
```

Note If you omit the **dlci** option for Frame Relay interfaces, the MAC address is mapped to the first DLCI circuit that is configured for the specified VLAN on that interface. Similarly, if you omit the **pvc** option for ATM interfaces, the MAC address is mapped to the first PVC that is configured for the specified VLAN on that interface. To ensure that the MAC address is configured correctly, we recommend that you always use the **dlci** and **pvc** keywords on the appropriate interfaces.

Examples

The following example shows how to add static entries to the MAC address table:

```
Device(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
```

The following example shows how to configure a static MAC address with IGMP snooping disabled for a specified address:

```
Device(config)#
mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7 disable-snooping
```

The following example shows how to add static entries to the MAC address table for an ATM PVC circuit and for a Frame Relay DLCI circuit:

```
Device(config)# mac-address-table static 0C01.0203.0405 vlan 101 interface ATM6/1 pvc 6/101
Device(config)# mac-address-table static 0C01.0203.0406 vlan 202 interface POS4/2 dlci 200
```

Related Commands

Command	Description
show mac-address-table address	Displays MAC address table information for a specific MAC address.

mac-address-table secure

To add secure addresses to the MAC address table, use the **mac-address-tablesecure** command in global configuration mode. To remove secure entries from the MAC address table, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

no mac-address-table secure *hw-address* **vlan** *vlan-id*

Catalyst Switches

mac-address-table secure *hw-address* [**atm** *slot/port***vlan** *vlan-id*]

no mac-address-table secure *hw-address* [**vlan** *vlan-id*]

Syntax Description

hw -address	MAC address that is added to the table.
interface	Port to which packets destined for *hw-address* are forwarded.
fa	Specifies FastEthernet.
gi	Specifies Gigabit Ethernet.
slot	(Optional) The slot (slot 1 or slot 2) to which to add dynamic addresses.
port	(Optional) Port interface number. The ranges are based on type of Ethernet switch network module used: • 0 to 15 for NM-16ESW • 0 to 35 for NM-36ESW • 0 to 1 for GigabitEthernet
atm *slot* / *port*	(Optional) Add secure addresses to the ATM module in slot 1 or 2. The port is always 0 for an ATM interface.

vlan *vlan -id*	Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers The *interface* and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded. The **vlan** keyword is optional if the port is a static-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. This keyword is required for multi-VLAN and trunk ports. The value of *vlan-id* is the ID of the VLAN to which secure entries are added. Valid IDs are 1 to 1005; do not enter leading zeroes. Catalyst Switches (Optional) The *interface* and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded. The **vlan** keyword is optional if the port is a static-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. This keyword is required for multi-VLAN and trunk ports. The value of *vlan-id* is the ID of the VLAN to which secure entries are added. Valid IDs are 1 to 1005; do not enter leading zeroes.

Command Default

Secure addresses are not added to the MAC address table.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2(8)SA	This command was introduced.
11.2(8)SA3	The **vlan** keyword was added.
11.2(8)SA5	The **atm** keyword was added.
12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T, on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Release	Modification
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
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 your feature set, platform, and platform hardware.

Usage Guidelines

Catalyst Switches

Secure addresses can be assigned to only one port at a time. Therefore, if a secure address table entry for the specified MAC address and VLAN already exists on another port, it is removed from that port and assigned to the specified one.

Dynamic-access ports cannot be configured with secure addresses.

Examples

The following example shows how to add a secure MAC address to VLAN 6 of port fa1/1:

Router(config)# mac-address-table secure 00c0.00a0.03fa fa1/1 vlan 6

Examples

The following example shows how to add a secure MAC address to VLAN 6 of port fa1/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa fa1/1 vlan 6
```

The following example shows how to add a secure MAC address to ATM port 2/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa atm 2/1
```

Related Commands

Command	Description
clear mac -address-table	Deletes entries from the MAC address table.
mac -address-tableaging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
mac -address-tabledynamic	Adds dynamic addresses to the MAC address table.
mac -address-tablestatic	Adds static addresses to the MAC address table.
show mac -address-table	Displays the MAC address table.

mls switching unicast

To enable the hardware switching of the unicast traffic for an interface, use the **mlsswitchingunicast** command in interface configuration mode. To disable the hardware switching of the unicast traffic for an interface, use the **no** form of this command.

mls switching unicast

no mls switching unicast

Syntax Description

This command has no arguments or keywords.

Command Default

Hardware switching of the unicast traffic for an interface is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

Examples

This example shows how to enable the hardware switching for an interface:

```
Router(config-if
)# mls switching unicast
Router(config-if)#
```

This example shows how to disable the hardware switching for an interface:

```
Router(config-if
)# no mls switching unicast
Router(config-if)#
```

Related Commands

Command	Description
mls switching	Enables hardware switching.

mode dot1q-in-dot1q access-gateway

To enable a Gigabit Ethernet WAN interface to act as a gateway for 802.1Q in 802.1Q (Q-in-Q) VLAN translation, use the **modedot1q-in-dot1qaccess-gateway**command. To disable the Q-in-Q VLAN translation on the interface, use the **no** form of this command.

mode dot1q-in-dot1q access-gateway

no mode dot1q-in-dot1q access-gateway

Syntax Description

This command has no arguments or keywords.

Command Default

A Gigabit Ethernet WAN interface does not act as a gateway for 802.1Q in 802.1Q (Q-in-Q) VLAN translation.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	Support was added for Q-in-Q link bundles using virtual port-channel interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on the Gigabit Ethernet (GE) WAN interfaces on Cisco 7600 series routers that are configured with an Optical Services Module (OSM)-2+4GE-WAN+ OSM module only.

OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32

802.1Q provides a trunking option that tags packets with two VLAN tags to allow multiple VLANs to be trunked together across an intermediate network. This use of a double-tagged tunnel is also referred to as Q-in-Q tunneling.

The **modedot1q-in-dot1qaccess-gateway**command enhances Q-in-Q tunneling by tagging packets with two VLAN tags to allow multiple VLANs to be trunked together across an intermediate network. This use of double-tagged tunnels performs the following functions:

- Switches packets that are tagged with two 802.1Q VLAN tags to a destination service based on the combination of VLAN tags.
- Supports traffic shaping based on the VLAN tags.
- Copies the 802.1P prioritization bits (P bits) from the inner (customer) VLAN tag to the outer (service provider) VLAN tag.

In Cisco IOS Release 12.2(18)SXE and later releases, you can also combine multiple GE-WAN interfaces into a virtual port-channel interface to enable Q-in-Q link bundling. Combining the interfaces not only simplifies the configuration, but allows the GE-WAN OSM to load balance the provider edge (PE) VLANs among the physical interfaces that are members of the bundle. Also, if one interface member of the link bundle goes down, its PE VLANs are automatically reallocated to the other members of the bundle.

Note You must remove all IP addresses that have been configured on the interface before using the **modedot1q-in-dot1qaccess-gateway**command.

After configuring the **modedot1q-in-dot1qaccess-gateway**command, use the **bridge-domain(subinterfaceconfiguration)**command to configure the VLAN mapping to be used on each subinterface.

Caution Using the **modedot1q-in-dot1qaccess-gateway**command on an interface automatically deletes all the subinterfaces that might be configured on the interface. It also releases any internal VLANs that might have been previously used on the interface and its subinterfaces, allowing them to be reused for Q-in-Q translation. The same situation occurs when using the **no** form of the command, which also deletes all subinterfaces and releases any VLANs that are currently being used by the interface and subinterface. We recommend that you save the interface configuration before entering the **modedot1q-in-dot1qaccess-gateway**command.

Note Port-channel interface counters (as shown by the **showcountersinterfaceport-channel** and **showinterfaceport-channelcounters** commands) are not supported for channel groups that are using GE-WAN interfaces for Q-in-Q link bundling. The **showinterfaceport-channel**{*number* | *number.subif* } command (without the **counters** keyword) is supported, however.

Tip The **mlsqostrust** command has no effect on a GE-WAN interface or port-channel group that has been configured with the **modedot1q-in-dot1qaccess-gateway**command. These interfaces and port channels always trust the VLAN class of service (CoS) bits in this configuration.

Examples

This example shows a typical configuration for the **modedot1q-in-dot1qaccess-gateway**command:

```
Router# configure terminal
Router(config)# interface GE-WAN 4/1
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

This example shows the system message that appears when you try to configure the **modedot1q-in-dot1qaccess-gateway**command without first removing the IP address configuration:

```
Router# configure terminal
Router(config)# interface GE-WAN 3/0
```

```
Router(config-if)# mode dot1q-in-dot1q access-gateway

% interface GE-WAN3/0 has IP address 192.168.100.101
configured. Please remove the IP address before configuring
'mode dot1q-in-dot1q access-gateway' on this interface.
Router(config-if)# no ip address 192.168.100.101 255.255.255

Router(config-if)# mode dot1q-in-dot1q access-gateway

Router(config-if)#
```

This example shows how to disable QinQ mapping on an interface by using the **no** form of the **modedot1q-in-dot1qaccess-gateway**command. In addition, this command automatically removes all subinterfaces on the interface and all of the subinterface QinQ mappings (configured with the **bridge-domain(subinterfaceconfiguration)**command) and service policies.

```
Router# configure terminal

Router(config)# interface GE-WAN 3/0

Router(config-if)# no mode dot1q-in-dot1q access-gateway

Router(config-if)#
```

This example shows a virtual port-channel interface that was created and assigned with two GE-WAN interfaces. The **modedot1q-in-dot1qaccess-gateway**command is then enabled on the port-channel interface to allow it to act as a QinQ link bundle:

```
Router(config)# interface port-channel 20

Router(config-if)# interface GE-WAN 3/0

Router(config-if)# port-channel 20 mode on

Router(config-if)# interface GE-WAN 3/1

Router(config-if)# port-channel 20 mode on

Router(config-if)# interface port-channel 20

Router(config-if)# no ip address

Router(config-if)# mode dot1q-in-dot1q access-gateway

Router(config-if)#
```

This example shows the error message that appears if you attempt to enable QinQ translation on a port-channel interface that contains one or more invalid interfaces:

```
Router# configure terminal

Router(config)# interface port-channel 30

7600-2(config-if)# mode dot1q-in-dot1q access-gateway

% 'mode dot1q-in-dot1q access-gateway' is not supported on Port-channel30
% Port-channel30 contains 2 Layer 2 Gigabit Ethernet interface(s)
Router(config-if)#
```

Related Commands

Command	Description
bridge-domain (subinterface configuration)	Binds a PVC to the specified VLAN ID.
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.

Command	Description
policy-map	Accesses QoS policy-map configuration mode to configure the QoS policy map.
service-policy	Attaches a policy map to an interface.
set cos cos-inner (policy-map configuration)	Sets the 802.1Q prioritization bits in the trunk VLAN tag of a Q-in-Q-translated outgoing packet with the priority value from the inner customer-edge VLAN tag.
show cwan qinq	Displays the inner, outer, and trunk VLANs that are used in Q-in-Q translation.
show cwan qinq bridge-domain	Displays the provider-edge VLAN IDs that are used on a Gigabit Ethernet WAN interface for Q-in-Q translation or to show the customer-edge VLANs that are used for a specific provider-edge VLAN.
show cwan qinq interface	Displays interface statistics for IEEE Q-in-Q translation on one or all Gigabit Ethernet WAN interfaces and port-channel interfaces.
show cwtlc qinq	Displays the information that is related to Q-in-Q translation and is contained in the XCM on board the supervisor engine.

name (MST)

To set the name of a Multiple Spanning Tree (MST) region, use the **name** command in MST configuration submode. To return to the default name, use the **no** form of this command.

name *name*

no name *name*

Syntax Description

name	Name to give the MST region. It can be any string with a maximum length of 32 characters.

Command Default

Empty string

Command Modes

MST configuration (config-mst)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
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 12.2(33)SRA.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

Two or more Cisco 7600 series routers with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.

Caution Be careful when using the **name** command to set the name of an MST region. If you make a mistake, you can put the Cisco 7600 series router in a different region. The configuration name is a case-sensitive parameter.

Examples

This example shows how to name a region:

```
Device(config-mst)# name Cisco
Device(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
revision	Sets the revision number for the MST configuration.
show	Verifies the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree mst configuration	Enters MST configuration submode.

port-channel load-defer

To configure the port load share deferral interval for all port channels, use the **port-channelload-defer** command in global configuration mode. To reset the port defer interval to the default setting, use the **no** form of this command.

port-channel load-defer *seconds*

no port-channel load-defer *seconds*

Syntax Description

seconds	Sets the time interval in seconds by which load sharing will be deferred on the switch. Valid range is from 1 to 1800 seconds. The default deferal interval is 120 seconds

Command Default

The port defer interval is 120 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(50)SY	This command was introduced. Added the *seconds* variable for use in Cisco IOS Release 12.2(50)SY.

Usage Guidelines

To reduce data loss following a stateful switchover (SSO), port load share deferral can be enabled by entering the **port-channelportload-defer** command on a port channel of a switch that is connected by a multichassis EtherChannel (MEC) to a virtual switching system (VSS). Port load share deferral temporarily prevents the switch from forwarding data traffic to MEC member ports on a failed chassis of the VSS while the VSS recovers from the SSO.

The load share deferral interval is determined by a single global timer configurable by the **port-channelload-defer** command. After an SSO switchover, a period of several seconds to several minutes can be required for the reinitialization of line cards and the reestablishment of forwarding tables, particularly multicast topologies.

The valid range of *seconds* is 1 to 1800 seconds; the default is 120 seconds.

Examples

This example shows how to set the global port deferral interval to 60 seconds:

```
Router(config)#
```

```
port-channel load-defer 60
Router(config)#
```

This example shows how to verify the configuration of the port deferral interval on a port channel:

```
Router# show etherchannel 50 port-channel

                Port-channels in the group:
                ----------------------
Port-channel: Po50    (Primary Aggregator)
------------
Age of the Port-channel   = 0d:00h:22m:20s
Logical slot/port   = 46/5          Number of ports = 3
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Fast-switchover     = disabled
Load share deferral = enabled   defer period = 60 sec
   time left = 57 sec
Router#
```

Related Commands

Command	Description
interface port-channel	Creates a port channel virtual interface and enters interface configuration mode.
port-channel port load-defer	Enables the port load share deferral feature on a port channel.
show etherchannel	Displays the EtherChannel information for a channel.

private-vlan

To configure private VLANs (PVLANs), use the **private-vlan** command in VLAN configuration mode. To remove the PVLAN configuration, use the **no** form of this command.

private-vlan {**isolated**| **community**| **primary**}

no private-vlan {**isolated**| **community**| **primary**}

Syntax Description

isolated	Designates the VLAN as an isolated PVLAN.
community	Designates the VLAN as a community PVLAN.
primary	Designates the VLAN as the primary PVLAN.

Command Default

No PVLANs are configured.

Command Modes

VLAN configuration (config-vlan)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was modified. A configuration restriction was added. See the “Usage Guidelines” section for additional information.
12.2(17d)SXB	This command was modified. 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 12.2(33)SRA.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

You cannot configure PVLANs on a port-security port. If you enter the **pvlan** command on a port-security port, the following error message is displayed:

```
Command rejected: Gix/y is Port Security enabled port.
```

Within groups of 12 ports (1-12, 13-24, 25-36, and 37-48), if one of the ports is a trunk, a Switch Port Analyzer (SPAN) destination, or a promiscuous PVLAN port, then do not configure the ports as isolated or as community VLAN ports. If so, any isolated or community VLAN configuration for the other ports within the 12 ports is inactive. To reactivate the ports, remove the isolated or community VLAN port configuration and enter the **shutdown** and **noshutdown** commands.

Caution If you enter the **shutdown** command and then the**noshutdown** command in the VLAN configuration mode on a PVLAN (primary or secondary), the PVLAN type and association information can be deleted. Ensure to reconfigure the VLAN as a PVLAN.

Note In Release 12.2(17a)SX, this restriction applies to Ethernet 10 Mb, 10/100 Mb, and 100 Mb modules except WS-X6548-RJ-45 and WS-X6548-RJ-21. In releases earlier than Release 12.2(17a)SX, this restriction applies to Ethernet 10 Mb, 10/100 Mb, and 100 Mb modules.

You cannot configure VLAN 1 or VLANs 1001 to 1005 as PVLANs.

VLAN Trunking Protocol (VTP) does not propagate PVLAN configuration. Each protected or private port is associated with a PVLAN, that is not supported through VTP. Therefore, you must configure PVLANs on each device where you require PVLAN ports.

A promiscuous port is a private port that is assigned to a primary VLAN.

An isolated VLAN is a VLAN that is used by isolated ports to communicate with promiscuous ports. The traffic from an isolated VLAN is blocked on all other private ports in the same VLAN. This traffic can only be received by standard trunking ports and promiscuous ports that are assigned to the corresponding primary VLAN.

A primary VLAN is the VLAN that is used to carry the traffic from the routers to customer end stations on private ports.

A community VLAN is the VLAN that carries the traffic among community ports, and from community ports to the promiscuous ports on the corresponding primary VLAN.

You can specify only one isolated *vlan-id*in the **vlan** command, while multiple community VLANs are allowed. Isolated and community VLANs can only be associated with one VLAN. The associated VLAN list must not contain primary VLANs. You cannot configure a VLAN that is already associated to a primary VLAN as a primary VLAN.

The **private-vlan** commands do not take effect until you exit the VLAN configuration mode.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive.

See the Cisco 7600 Series Router Cisco IOS Software Configuration Guide for additional configuration guidelines.

Examples

The following example shows how to configure VLAN 303 as a community LAN:

```
Router# configure terminal
Router(config)# vlan 303
Router(config-vlan)# private-vlan community
Router(config-vlan)# end
```

The following example shows how to configure VLAN 440 as an isolated VLAN:

```
Router# configure terminal
Router(config)# vlan 440
Router(config-vlan)# private-vlan isolated
Router(config-vlan)# end
```

The following example shows how to configure VLAN 233 as a primary LAN:

```
Router# configure terminal
Router(config)# vlan 233
Router(config-vlan)# private-vlan primary
Router(config-vlan)# end
```

The following example shows how to remove a PVLAN relationship and delete the primary VLAN. The associated secondary VLANs are not deleted.

```
Router(config-vlan)# no private-vlan
```

Related Commands

Command	Description
private-vlan association	Creates an association between PVLANs.
show vlan	Displays VLAN information.
show vlan private-vlan	Displays PVLAN information.
vlan (VLAN)	Configures a specific VLAN.