Cisco IOS LAN Switching Command Reference

November 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco IOS LAN Switching Command Reference

CONTENTS

Introduction

This document describes the commands used to configure LAN switching and multilayer switching features in Cisco IOS software.

The commands for configuring LAN Emulation (LANE) features are presented in the *Cisco IOS Asynchronous Transfer Mode Command Reference*.

Note Prior to Cisco IOS Release 12.4, the commands for configuring LANE, LAN switching, and multilayer switching features were presented in the *Cisco IOS IP Switching Command Reference*.

For Guidelines About Configuring this Cisco IOS Feature	Refer to the Following Cisco IOS Configuration Guide
LAN switching-related features	*Cisco IOS LAN Switching Configuration Guide*

LAN Switching Commands

bridge-domain

To enable RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI), use the **bridge-domain** command in Frame Relay DLCI configuration, interface configuration, interface ATM VC configuration, or PVC range configuration mode. To disable bridging, use the **no** form of this command.

bridge-domain *vlan-id* [**access** | **dot1q** [*tag*] | **dot1q-tunnel**] [**broadcast**] [**ignore-bpdu-pid**] [**pvst-tlv** *CE-vlan*] [**increment**] [**lan-fcs**] [**split-horizon**]

no bridge-domain *vlan-id*

Syntax Description

vlan-id	The number of the VLAN to be used in this bridging configuration. The valid range is from 2 to 4094.
access	(Optional) Enables bridging access mode, in which the bridged connection does not transmit or act upon bridge protocol data unit (BPDU) packets.
dot1q	(Optional) Enables Institute of Electrical and Electronic Engineers (IEEE) 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network. If this keyword is not specified, the ingress side assumes a CoS value of 0 for quality of service (QoS) purposes.
tag	(Optional—ATM PVCs only) Specifies the 802.1Q value in the range 1 to 4095. You can specify up to 32 **bridge-domain** command entries using **dot1q** *tag* for a single PVC. The highest tag value in a group of **bridge-domain** commands must be greater than the first tag entered (but no more than 32 greater).
dot1q-tunnel	(Optional) Enables IEEE 802.1Q tunneling mode, so that service providers can use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and segregating traffic in different customer VLANs.
broadcast	(Optional) Enables bridging broadcast mode on this PVC. This option is not supported for multipoint bridging. Support for this option was removed in Cisco IOS Release 12.2(18)SXF2 and Cisco IOS Release 12.2(33)SRA.
ignore-bpdu-pid	(Optional for ATM interfaces only) Ignores BPDU protocol identifiers (PIDs) and treats all BPDU packets as data packets to allow interoperation with ATM customer premises equipment (CPE) devices that do not distinguish BPDU packets from data packets.
pvst-tlv	(Optional) When the router or switch is transmitting, translates Per-VLAN Spanning Tree Plus (PVST+) BPDUs into IEEE BPDUs. When the router or switch is receiving, translates IEEE BPDUs into PVST+ BPDUs.
CE-vlan	Customer-edge VLAN in the Shared Spanning Tree Protocol (SSTP) tag-length-value (TLV) to be inserted in an IEEE BPDU to a PVST+ BPDU conversion.
increment	(PVC range configuration mode only) (Optional) Increments the bridge domain number for each PVC in the range.

lan-fcs	(Optional) Specifies that the VLAN bridging should preserve the Ethernet LAN frame checksum (FCS) of the Ethernet frames across the ATM network. **Note** This option applies only to routers using a FlexWAN module. Support for this option was removed in Cisco IOS Release 12.2(18)SXF2 and Cisco IOS Release 12.2(33)SRA.
split-horizon	(Optional) Enables RFC 1483 split horizon mode to globally prevent bridging between PVCs in the same VLAN.

Defaults

Bridging is disabled.

Command Modes

Frame Relay DLCI configuration (config-fr-dlci)
Interface configuration (config-if)—Only the **dot1q** and **dot1q-tunnel** keywords are supported in interface configuration mode.
Interface ATM VC configuration (config-if-atm-vc)
PVC range configuration (config-if-atm-range)

Command History

Release	Modification
12.1(13)E	This command was introduced as the **bridge-vlan** command for the 2-port OC-12 ATM WAN Optical Services Modules (OSMs) on Cisco 7600 series routers and Catalyst 6500 series switches.
12.1(12c)E	This command was integrated into Cisco IOS Release 12.1(12c)E.
12.1(14)E1	This command was integrated into Cisco IOS Release 12.1(14)E1. The **dot1q-tunnel** keyword was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. The **dot1q-tunnel** keyword is not supported in this release.
12.1(19)E	The **split-horizon** keyword was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S. The **dot1q-tunnel** and **split-horizon** keywords are supported in this release.
12.2(17a)SX	Support was added for the **dot1q-tunnel** keyword in Cisco IOS Release 12.2(17a)SX.
12.2(18)SXE	This command was renamed from **bridge-vlan** to **bridge-domain**. The **access**, **broadcast**, **ignore-bpdu-pid**, and **increment** keywords were added.
12.2(18)SXF2	Support for the **lan-fcs** and **broadcast** keywords was removed. The **ignore-bpdu-pid** and **pvst-tlv** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

RFC 1483 bridging on ATM interfaces supports the point-to-point bridging of Layer 2 packet data units (PDUs) over Ethernet networks. RFC 1490 Frame Relay bridging on Packet over SONET (POS) or serial interfaces that are configured for Frame Relay encapsulation provides bridging of Frame Relay packets over Ethernet networks.

The Cisco 7600 router can transmit BPDUs with a PID of either 0x00-0E or 0x00-07. When the router connects to a device that is fully compliant with RFC 1483 Appendix B, in which the IEEE BPDUs are sent and received by the other device using a PID of 0x00-0E, you must not use the **ignore-bpdu-pid** keyword.

If you do not enter the **ignore-bpdu-pid** keyword, the PVC between the devices operates in compliance with RFC 1483 Appendix B. This is referred to as *strict mode*. Entering the **ignore-bpdu-pid** keyword creates *loose mode*. Both modes are described as follows:

- Without the **ignore-bpdu-pid** keyword, in strict mode, IEEE BPDUs are sent out using a PID of 0x00-0E, which complies with RFC 1483.
- With the **ignore-bpdu-pid** keyword, in loose mode, IEEE BPDUs are sent out using a PID of 0x00-07, which is normally reserved for RFC 1483 data.

Cisco-proprietary PVST+ BPDUs are always sent out on data frames using a PID of 0x00-07, regardless of whether you enter the **ignore-bpdu-pid** keyword.

Use the **ignore-bpdu-pid** keyword when connecting to devices such as ATM digital subscriber line (DSL) modems that send PVST (or 802.1D) BPDUs with a PID of 0x00-07.

The **pvst-tlv** keyword enables BPDU translation when the router interoperates with devices that understand only PVST or IEEE Spanning Tree Protocol. Because the Catalyst 6500 series switch ATM modules support PVST+ only, you must use the **pvst-tlv** keyword when connecting to a Catalyst 5000 family switch that understands only PVST on its ATM modules, or when connecting with other Cisco IOS routers that understand IEEE format only.

When the router or switch is transmitting, the **pvst-tlv** keyword translates PVST+ BPDUs into IEEE BPDUs.

When the router or switch is receiving, the **pvst-tlv** keyword translates IEEE BPDUs into PVST+ BPDUs.

Note The **bridge-domain** and **bre-connect** commands are mutually exclusive. You cannot use both commands on the same PVC for concurrent RFC 1483 and BRE bridging.

To preserve class of service (CoS) information across the ATM network, use the **dot1q** option. This configuration uses IEEE 802.1Q tagging to preserve the VLAN ID and packet headers as they are transported across the ATM network.

To enable service providers to use a single VLAN to support customers that have multiple VLANs, while preserving customer VLAN IDs and segregating traffic in different customer VLANs, use the **dot1q-tunnel** option on the service provider router. Then use the **dot1q** option on the customer routers.

Note The **access**, **dot1q**, and **dot1q-tunnel** options are mutually exclusive. If you do not specify any of these options, the connection operates in "raw" bridging access mode, which is similar to access, except that the connection does act on and transmit BPDU packets.

RFC 1483 bridging is supported on AAL5-MUX and AAL5-LLC Subnetwork Access Protocol (SNAP) encapsulated PVCs. RFC-1483 bridged PVCs must terminate on the ATM interface, and the bridged traffic must be forwarded over an Ethernet interface, unless the **split-horizon** option is used, which allows bridging of traffic across bridged PVCs.

Note RFC 1483 bridging is not supported for switched virtual circuits (SVCs). It also cannot be configured for PVCs on the main interface.

In interface configuration mode, only the **dot1q** and **dot1q-tunnel** keyword options are supported.

Examples

The following example shows a PVC being configured for IEEE 802.1Q VLAN bridging using a VLAN ID of 99:

```
Router# configure terminal
Router(config)# interface ATM6/2
Router(config-if)# pvc 2/101
Router(config-if-atm-vc)# bridge-domain 99 dot1q
Router(config-if-atm-vc)# end
```

The following example shows how to enable BPDU translation when a Catalyst 6500 series switch is connected to a device that understands only IEEE BPDUs in an RFC 1483-compliant topology:

```
Router(config-if-atm-vc)# bridge-domain 100 pvst-tlv 150
```

The **ignore-bpdu-pid** keyword is not used because the device operates in an RFC 1483-compliant topology for IEEE BPDUs.

The following example shows how to enable BPDU translation when a Catalyst 5500 ATM module is a device that understands only PVST BPDUs in a non-RFC1483-compliant topology. When a Catalyst 6500 series switch is connected to a Catalyst 5500 ATM module, you must enter both keywords.

```
Router(config-if-atm-vc)# bridge-domain 100 ignore-bpdu-pid pvst-tlv 150
```

To enable BPDU translation for the Layer 2 Protocol Tunneling (L2PT) topologies, use the following command:

```
Router(config-if-atm-vc)# bridge-domain 100 dot1q-tunnel ignore-bpdu-pid pvst-tlv 150
```

The following example shows a range of PVCs being configured, with the bridge domain number being incremented for each PVC in the range:

```
Router(config)# interface atm 8/0.100
Router(config-if)# range pvc 102/100 102/199
Router(config-if-atm-range)# bridge-domain 102 increment
```

Related Commands

Command	Description
bre-connect	Enables the BRE over a PVC or SVC.
show atm pvc	Displays the configuration of a particular PVC.

bridge-domain (subinterface)

To enable bridging across Gigabit Ethernet subinterfaces, use the **bridge-domain** command in subinterface configuration mode. To disable bridging, use the **no** form of this command.

bridge-domain *vlan-id* {**dot1q** | **dot1q-tunnel**} [**bpdu** {**drop** | **transparent**}] [**split-horizon**]

no bridge-domain *vlan-id* {**dot1q** | **dot1q-tunnel**} [**bpdu** {**drop** | **transparent**}] [**split-horizon**]

Syntax Description

vlan-id	Specifies the number of the virtual LAN (VLAN) to be used in this bridging configuration. The valid range is from 2 to 4094.
dot1q	Enables IEEE 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network. If not specified, the ingress side assumes a CoS value of 0 for QoS purposes.
dot1q-tunnel	Enables IEEE 802.1Q tunneling mode, so that service providers can use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated.
bpdu {**drop** | **transparent**}	(Optional) Specifies whether or not BPDUs are processed or dropped: • **drop**—Specifies that BPDU packets are dropped on the subinterface. • **transparent**—Specifies that BPDU packets are forwarded as data on the subinterface, but not processed.
split-horizon	(Optional) Enables RFC 1483 split horizon mode to globally prevent bridging between PVCs in the same VLAN.

Defaults

Bridging is disabled.

Command Modes

Subinterface configuration (config-subif)

Command History

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

Usage Guidelines

This command has the following restrictions in Cisco IOS Release 12.2(33)SRA:

- The command is available on the Cisco 7600 SIP-400 with a 2-Port Gigabit Ethernet SPA only.
- You can place up to 120 subinterfaces in the same bridge domain on a single Cisco 7600 SIP-400.

To enable service providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated, use the **dot1q-tunnel** option on the service provider router. Then use the **dot1q** option on the customer routers.

Examples

The following example shows configuration of IEEE 802.1Q encapsulation for VLANs on Gigabit Ethernet subinterfaces with configuration of multipoint bridging (MPB). The MPB feature requires configuration of 802.1Q encapsulation on the subinterface.

The first subinterface bridges traffic on VLAN 100 and preserves CoS information in the packets by specifying the **dot1q** keyword.

```
Router(config)# interface GigabitEthernet 1/0/1.1
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# bridge-domain 100 dot1q
```

The second subinterface shows bridging of traffic on VLAN 200 in tunneling mode using the **dot1q-tunnel** keyword, which preserves the VLAN IDs of the bridged traffic.

```
Router(config)# interface GigabitEthernet 2/0/2.2
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# bridge-domain 200 dot1q-tunnel
```

The following example shows bridging of traffic from different VLANs on two separate Gigabit Ethernet subinterfaces into the same VLAN. First, the bridging VLAN 100 is created using the **vlan** command. Then, the Gigabit Ethernet subinterfaces implement IEEE 802.1Q encapsulation on VLAN 10 and VLAN 20 and bridge the traffic from those VLANs onto VLAN 100 using the **bridge-domain** command:

```
Router(config)# vlan 100
Router(config-vlan)# exit
!
Router(config)# interface GigabitEthernet 1/0/1.1
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# bridge-domain 100 dot1q
Router(config-subif)# exit
!
Router(config)# interface GigabitEthernet 1/0/2.1
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# bridge-domain 100 dot1q
```

Related Commands

Command	Description
encapsulation dot1q	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
vlan	Adds the specified VLAN IDs to the VLAN database and enters VLAN configuration mode.

bridge-vlan

To map a subinterface to specific inner customer-edge and outer provider-edge VLAN tags using 802.1Q-in-802.1Q (QinQ) translation, use the **bridge-vlan** command in subinterface configuration mode. To remove the QinQ VLAN mapping, use the **no** form of this command.

bridge-vlan *vlan-id* {**dot1q** | **dot1q-tunnel**} {*inner-vlan-id* | **out-range**}

no bridge-vlan *vlan-id* {**dot1q** | **dot1q-tunnel**} {*inner-vlan-id* | **out-range**}

Syntax Description

vlan-id	Outer provider-edge VLAN ID to be mapped; valid values are from 1 to 4094, except for the reserved IDs from 1002 through 1005.
dot1q	Specifies that the inner customer-edge and outer provider-edge VLAN tags on incoming packets are replaced with a single trunk VLAN tag on the outgoing Ethernet frames.
dot1q-tunnel	Specifies that the outer provider-edge VLAN tag on incoming packets is replaced with a trunk VLAN tag on the outgoing Ethernet frames.
inner-vlan-id	Inner customer-edge VLAN ID to be mapped; valid values are from 1 to 4094, except for the reserved IDs from 1002 through 1005.
out-range	Specifies that all customer-edge VLAN IDs that are outside of the range of 32 VLAN IDs are mapped for this provider-edge VLAN ID. See the "Usage Guidelines" section for additional information.

Defaults

- No bridged VLANs are configured.
- Packets with out-of-range or missing customer-edge VLANs are dropped.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was replaced by the **bridge-domain** (subinterface) command. See the "Usage Guidelines" section for more information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **bridge-vlan** command is supported only on subinterfaces of the Gigabit Ethernet WAN (GE-WAN) interfaces that are on the OSM-2+4GE-WAN+ OSM. The command cannot be used on other modules or on Gigabit Ethernet (GE) LAN interfaces.

You must have previously enabled QinQ translation on the main interface using the **mode dot1q-in-dot1q access-gateway** command before you can use the **bridge-vlan** command on a subinterface.

You must also use the **encapsulation dot1q** command on the subinterface to specify the trunk VLAN to use on outgoing packets.

Cisco IOS Release 12.2(18)SXE automatically replaces any use of the **bridge-vlan** command in previous QinQ configurations to the **bridge-domain** command.

Note When upgrading from Cisco IOS Release 12.2(18)SXD to Cisco IOS Release 12.2(18)SXE, be sure to save your running configuration to NVRAM using the **write memory** or **copy running-config startup-config** command so that you will save the QinQ configurations when you enter the **bridge-domain** command.

Each provider-edge VLAN supports a maximum of 32 customer-edge VLANs, which must be in a contiguous block that starts on a number divisible by 32 (for example: 0, 32, 64, and so forth). When you specify the first customer-edge VLAN ID for a provider-edge VLAN, the Cisco IOS software automatically associates the corresponding block of 32 IDs with that provider-edge VLAN.

VLAN 4095 is reserved and cannot be used as a customer-edge VLAN. Packets that contain a customer-edge VLAN ID of 4095 are automatically dropped by subinterfaces that are configured for QinQ translation. However, VLAN 4095 can continue to be used as a native (non-QinQ) VLAN.

A provider-edge VLAN cannot have the same ID as a native (non-QinQ) VLAN that is also being used on the router.

Entering the **dot1q** keyword results in QinQ translation, which is also known as a double-tag to single-tag translation.

When you enter the **dot1q-tunnel** keyword, the inner customer-edge tag is left unchanged. This results in transparent tunneling, which is also known as a double-tag to double-tag translation.

The **out-range** keyword is allowed only if you enter the **dot1q-tunnel** keyword.

You can use the **out-range** keyword to match the packets that do not have a customer-edge VLAN tag.

802.1Q provides for 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 called QinQ tunneling.

For additional information, refer to the *Optical Services Module Installation and Configuration Note*.

Examples

This example shows how to configure a double-tag-to-single-tag translation of packets that are tagged with both an inner customer-edge VLAN of 41 and an outer provider-edge VLAN of 33. The translated outgoing packets have a single trunk VLAN tag of 100.

```
Router# configure terminal
Router(config)# interface GE-WAN 4/1.100
Router(config-subif)# encapsulation dot1q 100
Router(config-subif)# bridge-vlan 33 dot1q 41
Router(config-subif)#
```

Note The above configuration also associates the block of 32 customer-edge VLANs ranging from 32 to 63 with provider-edge VLAN 33. All other customer-edge VLAN IDs are considered out of range.

This example shows how to configure a double-tag-to-double-tag translation of packets that are tagged with both an inner customer-edge VLAN of 109 and an outer provider-edge VLAN of 41. The translated outgoing packets have an inner customer-edge VLAN tag of 109 and an outer trunk VLAN tag of 203.

```
Router# configure terminal
Router(config)# interface GE-WAN 4/1.203
Router(config-subif)# encapsulation dot1q 203
Router(config-subif)# bridge-vlan 41 dot1q-tunnel 109
```

```
Router(config-subif)#
```

Note The above configuration also associates the block of 32 customer-edge VLANs ranging from 96 to 127 with provider-edge VLAN 41. All other customer-edge VLAN IDs are considered out of range.

This example shows how to configure a double-tag-to-double-tag translation of out-of-range packets. If this configuration is given together with the configuration shown above, this subinterface matches packets with an outer provider-edge VLAN of 41 and an inner customer-edge VLAN that is either missing, or that is in the range from 0 to 95 or from 128 to 4094. The translated outgoing packets keep the original out-of-range customer-edge VLAN as the inner VLAN and an outer trunk VLAN tag of 981.

```
Router# configure terminal
Router(config)# interface GE-WAN 4/1.1001
Router(config-subif)# encapsulation dot1q 981
Router(config-subif)# bridge-vlan 41 dot1q-tunnel out-range
Router(config-subif)#
```

This example shows the error message that appears when you attempt to specify the **out-range** keyword for a provider-edge VLAN before configuring at least one subinterface with a specific customer-edge VLAN ID for that same provider-edge VLAN:

```
Router# configure terminal
Router(config)# interface GE-WAN 4/1.1001
Router(config-subif)# bridge-vlan 2 dot1q-tunnel out-range

% bridge-vlan 2 does not have any inner-vlan configured.
out-of-range configuration needs at least one inner-vlan
defined to determine the range.

Router(config-subif)#
```

This example shows the system message that appears when you attempt to specify a VLAN ID that is already being used. In most cases, this message means that you have previously used this VLAN ID in another configuration or that the router has assigned this ID to an internal VLAN:

```
Router# configure terminal
Router(config)# interface GE-WAN 4/1.234
Router(config-subif)# bridge-vlan 123 dot1q 234

Command rejected: VLAN 123 not available

Router(config-subif)#
```

Tip To display a list of the internal VLANs that are currently in use on the router, use the **show vlan internal usage** command.

Related Commands

Command	Description
class-map	Accesses the QoS class-map configuration mode to configure QoS class maps.
encapsulation dot1q	Specifies the trunk VLAN to use on outgoing packets.
mode dot1q-in-dot1q access-gateway	Enables a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation.
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 QinQ-translated outgoing packet.
show cwan qinq	Displays the inner, outer, and trunk VLANs that are used in QinQ translation.
show cwan qinq bridge-domain	Displays the provider-edge VLAN IDs that are used on a Gigabit Ethernet WAN interface for QinQ 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 802.1Q-in-802.1Q (QinQ) translation on one or all Gigabit Ethernet WAN interfaces and port-channel interfaces.
show vlan internal usage	Displays a list of the internal VLANs that are currently in use on the router.

clear gvrp statistics

To clear Generic VLAN Registration Protocol (GVRP)-related statistics recorded on one or all GVRP enabled ports, use the **clear gvrp statistics** command in privileged EXEC mode.

clear gvrp statistics [**interface** *number*]

Syntax Description

interface *number*	(Optional) Displays GVRP information based on a specific interface.

Command Default

All GVRP statistics are removed.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to clear GVRP statistics on all GRVP enabled ports:

```
Router# clear gvrp statistics
```

Related Commands

Command	Description
debug gvrp	Displays GVRP debugging information.

clear mac-address-table

To remove a specified address (or set of addresses) from the MAC address table, use the **clear mac-address-table** command in privileged EXEC mode.

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

clear mac-address-table [**dynamic** | **secure** | **static**] [**address** *mac-address*] [**interface** *type slot/port*]

Using Catalyst Switches

clear mac-address-table [**dynamic** | **restricted static** | **permanent**] [**address** *mac-address*] [**interface** *type module port*]

clear mac-address-table notification mac-move counter [*vlan*]

Clearing a Dynamic Address using a Supervisor 720

clear mac-address-table dynamic [**address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id*]

Clearing a Dynamic Address using a a Supervisor Engine 2

clear mac-address-table dynamic [**address** *mac-address* | **interface** *interface-type interface-number* | **protocol** {**assigned** | **ip** | **ipx** | **other** } [**vlan** *vlan-id*]

Syntax Description

dynamic	(Optional) Clears only dynamic addresses.
secure	(Optional) Clears only secure addresses.
static	(Optional) Clears only static addresses.
restricted static	(Optional) Clears only restricted static addresses.
permanent	(Optional) Clears only permanent addresses.
address	(Optional) Clears only a specified address.
mac-address	(Optional) Specifies the MAC address.
interface	(Optional) Clears all addresses for an interface.
type	(Optional) Interface type: ethernet, fastethernet, fddi, atm, or port channel.
slot	(Optional) The module interface number.
interface-type interface-number	(Optional) Module and port number. The see the “Usage Guidelines” section for valid values.
notification mac-move counter	Clears the MAC-move notification counters.
vlan	(Optional) Specifies the VLAN to clear the MAC-move notification counters.
protocol assigned	(Optional) Specifies the assigned protocol accounts for such protocols such as DECnet, Banyan VINES, and AppleTalk.
protocol ip | **ipx**	(Optional) Specifies the protocol type of the entries to clear.

protocol other	(Optional) Specifies the protocol types (other than IP or IPX) of the entries to clear.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
module	(Optional) The module interface number: • 0 for fixed • 1 or A for module A • 2 or B for module B
port	(Optional) **Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers** Port interface number ranges 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 Gigabit Ethernet **Catalyst Switches** Port interface number ranging from 1 to 28: • 1 to 25 for Ethernet (fixed) • 26, 27 for Fast Ethernet (fixed) • Port channel

Command Default

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

All MAC addresses on the router being configured are cleared.

Using Catalyst Switches

The dynamic addresses are cleared.

Clearing a Dynamic Address

This command has no defaults in this mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
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	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 Cisco IOS Release 12.2(17d)SXB.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was changed to add the **notification mac-move counter** [*vlan*] keywords and argument.

Usage Guidelines

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

If the **clear mac-address-table** command is invoked with no options, all MAC addresses are removed. If you specify an address but do not specify an interface, the address is deleted from all interfaces. If you specify an interface but do not specify an address, all addresses on the specified interface are removed.

Using Catalyst Switches

If the **clear mac-address-table** command is invoked with no options, all dynamic addresses are removed. If you specify an address but do not specify an interface, the address is deleted from all interfaces. If you specify an interface but do not specify an address, all addresses on the specified interface are removed.

If a targeted address is not present in the MAC forwarding table, the following error message appears:

```
MAC address not found
```

Clearing a Dynamic Address

The valid values for the *interface* argument include the **ge-wan**, **atm**, and **pos** keywords that are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **protocol** {**assigned** | **ip** | **ipx** | **other**} keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

Enter the **clear mac-address-table dynamic** command to remove all dynamic entries from the table.

The following values are valid for *interface-type*:

- fastethernet
- gigabitethernet
- port-channel

Setting the Module and Port

The *interface-number* argument designates the module and port number. Valid values for *interface-number* 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.

Examples

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

The following example shows how to clear all dynamic addresses in the MAC forwarding table:

```
Router# clear mac-address-table dynamic
```

The following example shows how to clear the static address 0040.C80A.2F07 on Ethernet port 1:

```
Router# clear mac-address-table static address 0040.C80A.2F07 interface ethernet 0/1
```

Using Catalyst Switches

The following example shows how to clear all dynamic addresses in the MAC forwarding table:

```
Router# clear mac-address-table dynamic
```

The following example shows how to clear the MAC-move notification counters on a specific VLAN:

```
Router# clear mac-address-table notification mac-move counter 202
```

The following example shows the permanent address 0040.C80A.2F07 being cleared on Ethernet port 1:

```
Router# clear mac-address-table permanent address 0040.C80A.2F07 interface ethernet 0/1
```

Clearing a Dynamic Address on a 7600 using a Supervisor Engine 2

This example shows how to clear all dynamic Layer 2 entries for a specific interface (abc) and protocol type (IPX):

```
Router# clear mac-address-table dynamic interface abc protocol ipx
```

Related Commands

Command	Description
mac-address-table aging-time	Configures the length of time the switch keeps dynamic MAC addresses in memory before discarding.
mac-address-table permanent	Associates a permanent unicast or multicast MAC address with a particular switched port interface.
mac-address-table restricted static	Associates a restricted static address with a particular switched port interface.
mac-address-table secure	Associates a secure static address with a particular switched port interface.
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.
show mac-address-table	Displays addresses in the MAC address table for a switched port or module.
show mac-address-table secure	Displays the addressing security configuration.
show mac-address-table security	Displays the addressing security configuration.

clear mvrp statistics

To clear statistics related to Multiple VLAN Registration Protocol (MVRP) and recorded on one (or all) MVRP-enabled ports, use the **clear mvrp statistics** command in privileged EXEC configuration mode.

clear mvrp statistics [**interface** *interface*]

Syntax Description

interface	(Optional) Specifies an interface for which collected statistics will be cleared.
interface	(Optional) Indicates the interface number for which statistics will be cleared.

Command Default

Previously collected statistics are retained.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to clear collected statistics for MVRP-enabled devices or interfaces. If used without the **interface** keyword, the command clears all MVRP statistics on the device.

Examples

The following example clears collected MVRP statistics on a specified interface:

```
Router# clear mvrp statistics interface e0
```

Related Commands

Command	Description
show mvrp interface	Displays collected statistics for MVRP-enabled interfaces.

clear pagp

To clear the port-channel information, use the **clear pagp** command in privileged EXEC mode.

clear pagp {*group-number* | **counters**}

Syntax Description

group-number	Channel group number; valid values are a maximum of 64 values from 1 to 256.
counters	Clears traffic filters.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	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.

Examples

This example shows how to clear the port-channel information for a specific group:

```
Router# clear pagp 324
```

This example shows how to clear the port-channel traffic filters:

```
Router# clear pagp counters
```

Related Commands

Command	Description
show pagp	Displays port-channel information.

clear spanning-tree detected-protocol

To restart the protocol migration process, use the **clear spanning-tree detected-protocol** command in privileged EXEC mode.

clear spanning-tree detected-protocol [**interface** [*interface-type interface-number* | **port-channel** *pc-number* | **vlan** *vlan-interface*]

Syntax Description

interface	(Optional) Specifies the interface
interface-type	The type of interface that you want to clear the detected spanning tree protocol for.
interface-number	The of the interface that you want to clear the detected spanning tree protocol for.
port-channel	Clears the detected spanning tree protocol for a port-channel.
pc-number	Specifies the port channel interface. Range: 1 to 282.
vlan	Clears the detected spanning tree protocol for a VLAN.
vlan-interface	Specifies the VLAN interface. Range: 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

RSTP and MST have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a bridge running RSTP can send 802.1D BPDUs on one of its ports when it is connected to a legacy bridge. An MST bridge can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region. These mechanisms are not always able to revert to the most efficient mode. For example, an RSTP bridge that is designated for a legacy 802.1D stays in 802.1D mode even after the legacy bridge has been removed from the link. Similarly, an MST port assumes that it is a boundary port when the bridges to which it is connected have joined the same region. To force the MST port to renegotiate with the neighbors, enter the **clear spanning-tree detected-protocol** command.

If you enter the **clear spanning-tree detected-protocol** command with no arguments, the command is applied to every port of the Catalyst 6500 series switch.

Examples

This example shows how to restart the protocol migration on a specific interface:

```
Router# clear spanning-tree detected-protocol fa1/1
Router#
```

Related Commands

Command	Description
show spanning-tree mst	Displays information about the MST protocol.

clear vlan

To delete an existing VLAN from a management domain, use the **clear vlan** command in privileged EXEC mode.

clear vlan *vlan*

Syntax Description

vlan	Number of the VLAN. Valid values are 2 to 1000.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0	This command was introduced.
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

Follow these guidelines for deleting VLANs:

- When you delete an Ethernet VLAN in Virtual Trunking Protocol (VTP) server mode, the VLAN is removed from all switches in the same VTP domain.
- When you delete a VLAN in VTP transparent mode, the VLAN is deleted only on the current switch.
- To delete a Token Ring Bridge Relay Function (TRBRF) VLAN, you must either first reassign its child Token Ring Concentrator Relay Functions (TRCRFs) to another parent TRBRF or delete the child TRCRFs.

Caution When you clear a VLAN, all ports assigned to that VLAN become inactive. However, the VLAN port assignments are retained until you move the ports to another VLAN. If the cleared VLAN is reactivated, all ports still configured on that VLAN are also reactivated. A warning is displayed if you clear a VLAN that exists in the mapping table.

Examples

The following example shows how to clear an existing VLAN (VLAN 4) from a management domain:

```
Router# clear vlan 4
This command will deactivate all ports on vlan 4
in the entire management domain
Do you want to continue(y/n) [n]? y
VLAN 4 deleted
```

Related Commands

Command	Description
set vlan	Groups ports into a VLAN.
show vlans	Displays VLAN subinterfaces.

clear vlan counters

To clear the software-cached counter values to start from zero again for a specified VLAN or all existing VLANs, use the **clear vlan counters** command in privileged EXEC mode.

clear vlan [*vlan-id*] **counters**

Syntax Description

vlan-id	(Optional) The ID of a specific VLAN. Range: 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

If you do not specify a *vlan-id*; the software-cached counter values for all existing VLANs are cleared.

Examples

This example shows how to clear the software-cached counter values for a specific VLAN:

```
Router# clear vlan 10 counters
Clear "show vlan" counters on this vlan [confirm]y
Router#
```

Related Commands

Command	Description
show vlan counters	Displays the software-cached counter values.

clear vlan mapping

To delete existing 802.1Q virtual LAN (VLAN) to Inter-Switch Link (ISL) VLAN-mapped pairs, use the **clear vlan mapping** command in privileged EXEC mode.

clear vlan mapping dot1q {*1q-vlan* | **all**}

Syntax Description

dot1q	Specifies the 802.1Q VLAN.
1q-vlan	Number of the 802.1Q VLAN for which to remove the mapping.
all	Clears the mapping table of all entries.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0	This command was introduced.
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.

Examples

The following example shows how to clear an existing mapped 802.1Q VLAN (VLAN 1044) from the mapping table:

```
Router# clear vlan mapping dot1q 1044
Vlan Mapping 1044 Deleted.
```

The following example shows how to clear all mapped 802.1Q VLANs from the mapping table:

```
Router# clear vlan mapping dot1q all
All Vlan Mapping Deleted.
```

Related Commands

Command	Description
set vlan mapping	Maps 802.1Q VLANs to ISL VLANs.
show vlan mapping	Displays VLAN mapping table information.

clear vlan statistics

To remove virtual LAN (VLAN) statistics from any statically or system-configured entries, use the **clear vlan statistics** command in privileged EXEC mode.

clear vlan statistics

Syntax Description

This command has no arguments or keywords.

Defaults

VLAN statistics are not removed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
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.

Examples

The following example clears VLAN statistics:

```
Router# clear vlan statistics
```

Related Commands

Command	Description
show vlan counters	Displays the software-cached counter values.

clear vtp counters

To clear VLAN Trunk Protocol (VTP) counters, use the **clear vtp counters** command in privileged EXEC mode.

clear vtp counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRE.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to clear VTP counters:

```
Router# clear vtp counters
```

Related Commands

Command	Description
show vtp	Displays general information about the VTP management domain, status, and counters.
vtp	Configures the global VTP state.

collect top counters interface

To list the TopN processes and specific TopN reports, use the **collect top counters interface** command in user EXEC or privileged EXEC mode.

collect top [*number*] **counters interface** *interface-type* [**interval** *seconds*] [**sort-by** *sort-by-value*]

Syntax Description

number	(Optional) Number of ports to be displayed; valid values are from 1 to 5000 physical ports. The default is 20 physical ports.
interface-type	Type of ports to be used in the TopN request; valid values are **all**, **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **layer-2** *vlan-num*, and **layer-3**. The default is **all**. The **layer-2** *vlan-num* keyword and argument represents the number of Layer 2 interfaces. Range:1 to 4094.
interval *seconds*	(Optional) Specifies the interval over which the statistics are gathered. Range: 0 to 999 seconds. The default is 30 seconds.
sort-by *sort-by-value*	Specifies the port statistic to generate the report on; valid values are as follows: • **broadcast**—Sorts the report based on the receive and transmit broadcast packets. • **bytes**—Sorts the report based on the receive and transmit bytes. • **errors**—Sorts the report based on the receive errors. • **multicast**—Sorts the report based on the receive and transmit multicast packets. • **overflow**—Sorts the report based on the transmit overflow errors. • **packets**—Sorts the report based on the receive and transmit packets. • **utilization**—Sorts the report based on the port utilization. This is the default.

Defaults

The defaults are as follows:

- *number* is **20** physical ports.
- *interface-type* is **all**.
- *seconds* is **30** seconds.
- *sort-by-value* is **utilization**.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE	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 supported on Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet ports only. LAN ports on the OSMs are also supported.

If you specify an interval of **0** seconds, the TopN report is generated based on the absolute counters value.

Specifying the **interval** *seconds* keyword and the *sort-by-value* argument when the sorting criteria is **utilization** will not return a valid report because utilization can only be computed over an interval. For example, this syntax–**collect top counters interface fastEthernet sort-by utilization interval** *45*, will not generate a valid report.

Only a TopN task with a done status is allowed to display the report. If you try to view a report that is incomplete (pending), an appropriate message is displayed.

The TopN utility collects the following port utilization data for each physical port over the *seconds* interval:

- Total number of in and out bytes
- Total number of in and out packets
- Total number of in and out broadcast packets
- Total number of in and out multicast packets
- Total number of in errors (Ethernet ports such as CRC, undersize packets (+Runt), oversize packets, fragmentation, and jabber)
- Total number of buffer-overflow errors (including outlost packets; for example, transmit errors that are due to the buffer full and Ethernet ports: dmaTxOverflow and dmaTxFull)

After the collection of information, the ports are sorted according to the *sort-by-value* argument, and the top *number* of ports are displayed.

When the TopN reports are ready, a syslog message is displayed that the TopN reports are available. You can use the **show top interface report** command to view the reports. You can display the TopN reports multiple times until you enter the **clear top interface report** command to clear the reports.

Use the **clear top interface report** command to clear the reports.

Examples

This example shows how to sort the TopN report based on the receive and transmit broadcast packets:

```
Router# collect top 40 counters interface all sort-by broadcast
Router#
```

This example shows how to sort the TopN report based on the receive and transmit broadcast packets and specify the TopN sampling interval:

```
Router# collect top 40 counters interface all interval 500 sort-by broadcast
Router#
```

Related Commands

Command	Description
clear top counters interface report	Clears the TopN reports.
show top counters interface report	Displays TopN reports and information.

dot1q tunneling ethertype

To define the Ethertype field type used by peer devices when implementing Q-in-Q VLAN tagging, use the **dot1q tunneling ethertype** command in interface configuration mode. To remove the VLAN tag Ethertype, use the **no** form of this command.

dot1q tunneling ethertype {*0x88A8* | *0x9100* | *0x9200*}

no dot1q tunneling ethertype

Syntax Description

0x88A8 | *0x9100* | *0x9200*	Type of Ethertype field.

Defaults

The Ethertype field used by peer devices when implementing Q-in-Q VLAN tagging is 0x8100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(7)XI1	This command was implemented on the Cisco 10000 series routers.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

Use the **dot1q tunneling ethertype** command if the peer switching devices are using an Ethertype field value of 0x9100 or 0x9200. All Cisco switching devices use the default Ethertype field value of 0x88A8. The Cisco 10000 series router also supports the 0x9200 Ethertype field value.

Note On the Cisco 10000 series router, the Ethertype field for the outer VLAN ID can be changed, but the Ethertype field for the inner VLAN ID cannot be changed.

This command is used with the IEEE 802.1Q-in-Q VLAN Tag Termination feature in which double VLAN tagging is configured using the **encapsulation dot1q** command. 802.1Q double tagging allows a service provider to use a single VLAN to support customers who have multiple VLANs.

Examples

The following example shows how to configure an Ethertype field as 0x9100:

```
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# dot1q tunneling ethertype 0x9100
```

The following example shows how to configure an Ethertype field as 0x9200 on a Cisco 10000 series router:

```
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# dot1q tunneling ethertype 0x9200
```

Related Commands

Command	Description
encapsulation dot1q	Enables 802.1Q encapsulation of traffic on a specified subinterface or range of subinterfaces.
interface	Configures an interface and enters interface configuration mode.

encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN, use the **encapsulation dot1q** command in interface range configuration mode or subinterface configuration mode. To disable IEEE 802.1Q encapsulation, use the **no** form of this command.

Interface Range Configuration Mode

encapsulation dot1q *vlan-id* **second-dot1q** {**any** | *vlan-id*} [**native**]

no encapsulation dot1q

Subinterface Configuration Mode

encapsulation dot1q *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id*-*vlan-id*[,*vlan-id*-*vlan-id*]}

no encapsulation dot1q *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id*-*vlan-id*[,*vlan-id*-*vlan-id*]}

Syntax Description

vlan-id	Virtual LAN identifier. The allowed range is from 1 to 4094. For the IEEE 802.1Q-in-Q VLAN Tag Termination feature, the first instance of this argument defines the outer VLAN ID, and the second and subsequent instances define the inner VLAN ID.
native	(Optional) Sets the VLAN ID value of the port to the value specified by the *vlan-id* argument. **Note** This keyword is not supported by the IEEE 802.1Q-in-Q VLAN Tag Termination feature.
second-dot1q	Supports the IEEE 802.1Q-in-Q VLAN Tag Termination feature by allowing an inner VLAN ID to be configured.
any	Sets the inner VLAN ID value to a number that is not configured on any other subinterface. **Note** The **any** keyword in the **second-dot1q** command is not supported on a subinterface configured for IP over Q-in-Q (IPoQ-in-Q) because IP routing is not supported on ambiguous subinterfaces.
-	Separates the inner and outer VLAN ID values in the range to be defined. The hyphen is required.
,	Separates each VLAN ID range from the next range. The comma is required. Do not insert spaces between the values.

Defaults

IEEE 802.1Q encapsulation is disabled.

Command Modes

Interface range configuration (config-int-range)
Subinterface configuration (config-ifsub)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The **native** keyword was added.
12.2(2)DD	Support was added for this command in interface range configuration mode.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(7)T	The **second-dot1q** keyword was added to support the IEEE 802.1Q-in-Q VLAN Tag Termination feature.
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI and implemented on the Cisco 10000 series routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

Interface Range Configuration Mode

IEEE 802.1Q encapsulation is configurable on Fast Ethernet interfaces. IEEE 802.1Q is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

Use the **encapsulation dot1q** command in interface range configuration mode to apply a VLAN ID to each subinterface within the range specified by the **interface range** command. The VLAN ID specified by the *vlan-id* argument is applied to the first subinterface in the range. Each subsequent interface is assigned a VLAN ID, which is the specified *vlan-id* value plus the subinterface number minus the first subinterface number (VLAN ID + subinterface number – first subinterface number).

Note The Cisco 10000 series router does not support the **interface range** command nor the interface range configuration mode.

Do not configure encapsulation on the native VLAN of an IEEE 802.1Q trunk without using the **native** keyword. (Always use the **native** keyword when *vlan-id* is the ID of the IEEE 802.1Q native VLAN.)

Subinterface Configuration Mode

Use the **second-dot1q** keyword to configure the IEEE 802.1Q-in-Q VLAN Tag Termination feature. 802.1Q in 802.1Q (Q-in-Q) VLAN tag termination adds another layer of 802.1Q tag (called "metro tag" or "PE-VLAN") to the 802.1Q tagged packets that enter the network. Double tagging expands the VLAN space, allowing service providers to offer certain services such as Internet access on specific VLANs for some customers and other types of services on other VLANs for other customers.

After a subinterface is defined, use the **encapsulation dot1q** command to add outer and inner VLAN ID tags to allow one VLAN to support multiple VLANs. You can assign a specific inner VLAN ID to the subinterface; that subinterface is unambiguous. Or you can assign a range or ranges of inner VLAN IDs to the subinterface; that subinterface is ambiguous.

Examples

The following example shows how to create the subinterfaces within the range 0.11 and 0.60 and apply VLAN ID 101 to the Fast Ethernet0/0.11 subinterface, VLAN ID 102 to Fast Ethernet0/0.12 (*vlan-id* = 101 + 12 – 11 = 102), and so on up to VLAN ID 150 to Fast Ethernet0/0.60 (*vlan-id* = 101 + 60 – 11 = 150):

```
Router(config)# interface range fastethernet0/0.11 - fastethernet0/0.60
Router(config-int-range)# encapsulation dot1q 101
```

The following example shows how to terminate a Q-in-Q frame on an unambiguous subinterface with an outer VLAN ID of 100 and an inner VLAN ID of 200:

```
Router(config)# interface gigabitethernet1/0/0.1
Router(config-subif)# encapsulation dot1q 100 second-dot1q 200
```

The following example shows how to terminate a Q-in-Q frame on an ambiguous subinterface with an outer VLAN ID of 100 and an inner VLAN ID in the range from 100 to 199 or from 201 to 600:

```
Router(config)# interface gigabitethernet1/0/0.1
Router(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600
```

Related Commands

Command	Description
encapsulation isl	Enables the ISL, which is a Cisco proprietary protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches.
encapsulation sde	Enables IEEE 802.10 encapsulation of traffic on a specified subinterface in VLANs.
interface range	Specifies multiple subinterfaces on which subsequent commands are executed at the same time.
show vlans dot1q	Displays information about 802.1Q VLAN subinterfaces.

encapsulation isl

To enable the Inter-Switch Link (ISL), use the **encapsulation isl** command in subinterface configuration mode. To disable the ISL, use the **no** form of this command.

encapsulation isl *vlan-identifier*

no encapsulation isl *vlan-identifier*

Syntax Description

vlan-identifier	Virtual LAN (VLAN) identifier. Valid values on all platforms except the Cisco 7600 series are from 1 to 1000. On the Cisco 7600 series, valid values are from 1 to 4096.

Command Default

ISL is disabled.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
11.1	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

ISL is a Cisco protocol for interconnecting multiple switches and routers, and for defining VLAN topologies.

ISL encapsulation is configurable on Fast Ethernet interfaces.

ISL encapsulation adds a 26-byte header to the beginning of the Ethernet frame. The header contains a 10-bit VLAN identifier that conveys VLAN membership identities between switches.

To enter the subinterface configuration mode, you must enter the interface configuration mode first and then enter the **interface** command to specify a subinterface.

Examples

The following example shows how to enable ISL on Fast Ethernet subinterface 2/1.20:

```
Router(config)# interface FastEthernet 2/1.20
Router(config-subif)# encapsulation isl 400
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
show bridge vlan	Displays virtual LAN subinterfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show vlans	Displays VLAN subinterfaces.

encapsulation sde

To enable IEEE 802.10 encapsulation of traffic on a specified subinterface in virtual LANs (VLANs), use the **encapsulation sde** command in subinterface configuration mode. To disable IEEE 802.10 encapsulation, use the **no** form of this command.

encapsulation sde *sa-id*

no encapsulation sde *sa-id*

Syntax Description

sa-id	Security association identifier. This value is used as the VLAN identifier. The valid range is from 0 to 0xFFFFFFFE.

Command Default

IEEE 802.10 encapsulation is disabled.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
10.3	This command was introduced.
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

IEEE 802.10 is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

Secure Data Exchange (SDE) encapsulation is configurable only on the following interface types:

- IEEE 802.10 routing: FDDI
- IEEE 802.10 transparent bridging:
  - Ethernet
  - FDDI
  - HDLC serial
  - Transparent mode
  - Token Ring

Examples

The following example shows how to enable SDE on FDDI subinterface 2/0.1 and assigns a VLAN identifier of 9999:

```
Router(config)# interface fddi 2/0.1
Router(config-subif)# encapsulation sde 9999
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show vlans	Displays VLAN subinterfaces.

flowcontrol

To set the method of data flow control between the terminal or other serial device and the router, use the **flowcontrol** command in line configuration mode. To disable flow control, use the **no** form of this command.

flowcontrol {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}

no flowcontrol {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}

Catalyst 6500 Series Switches and Cisco 7600 Series Routers

To configure a port to send or receive pause frames, use the **flowcontrol** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

flowcontrol {**send** | **receive**} {**desired** | **off** | **on**}

no flowcontrol {**send** | **receive**} {**desired** | **off** | **on**}

Cisco uBR10012 Universal Broadband Router

To temporarily stop the transmission of data between two peers to prevent packet drops in the event of data overflow, use the **flowcontrol** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

flowcontrol receive off

no flowcontrol receive off

Syntax Description

none	Turns off flow control.
software	Sets software flow control.
lock	(Optional) Makes it impossible to turn off flow control from the remote host when the connected device *needs* software flow control. This option applies to connections using the Telnet or rlogin protocols.
[**in** | **out**]	(Optional) Specifies the direction of software or hardware flow control: the keyword **in** causes the Cisco IOS software to listen to flow control from the attached device, and the **out** keyword causes the software to send flow control information to the attached device. If you do not specify a direction, both directions are assumed.
hardware	Sets hardware flow control. For more information about hardware flow control, see the hardware manual that was shipped with your router.
Catalyst 6500 Series Switches and Cisco 7600 Series Routers	
send	Specifies that a port sends pause frames.
receive	Specifies that a port processes pause frames.
desired	Obtains predictable results regardless of whether a remote port is set to **on**, **off**, or **desired**.
off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.

Command Default

Flow control is disabled.

Catalyst 6500 Series Switches and Cisco 7600 Routers

Flow-control defaults depend upon port speed. The defaults are as follows:

- Gigabit Ethernet ports default to **off** for receive and **desired** for send.
- Fast Ethernet ports default to **off** for receive and **on** for send.
- On the 24-port 100BASE-FX and 48-port 10/100 BASE-TX RJ-45 modules, the default is **off** for receive and **off** for send.
- You cannot configure how WS-X6502-10GE 10-Gigabit Ethernet ports respond to pause frames. WS-X6502-10GE 10-Gigabit Ethernet ports are permanently configured to respond to pause frames.

Cisco uBR10012 Universal Broadband Router

Flow control is enabled by default.

Command Modes

Line configuration

Catalyst 6500 Series Switches, Cisco 7600 Series Routers, and Cisco uBR10012 Universal Broadband Router

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Catalyst 6500 Series Switches and Cisco 7600 Series Routers	
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)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

When software flow control is set, the default stop and start characters are Ctrl-S and Ctrl-Q (XOFF and XON). You can change them using the **stop-character** and **start-character** commands.

If a remote Telnet device requires software flow control, the remote system should not be able to turn it off. Using the **lock** option makes it possible to refuse “dangerous” Telnet negotiations if they are inappropriate.

Catalyst 6500 Series Switches and Cisco 7600 Series Routers

The **send** and **desired** keywords are supported on Gigabit Ethernet ports only.

Pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

Gigabit Ethernet ports on the Catalyst 6500 series switches and on the Cisco 7600 series routers use flow control to inhibit the transmission of packets to the port for a period of time; other Ethernet ports use flow control to respond to flow-control requests.

If a Gigabit Ethernet port receive buffer becomes full, the port transmits a "pause" packet that tells remote ports to delay sending more packets for a specified period of time. All Ethernet ports (1000 Mbps, 100 Mbps, and 10 Mbps) can receive and act upon "pause" packets from other devices.

You can configure non-Gigabit Ethernet ports to ignore received pause frames (**disable**) or to react to them (**enable**).

When used with **receive**, the **on** and **desired** keywords have the same result.

All the Gigabit Ethernet ports on the Catalyst 6500 series switches and the Cisco 7600 series routers can receive and process pause frames from remote devices.

To obtain predictable results, follow these guidelines:

- Use **send on** only when remote ports are set to **receive on** or **receive desired**.
- Use **send off** only when remote ports are set to **receive off** or **receive desired**.
- Use **receive on** only when remote ports are set to **send on** or **send desired**.
- Use **send off** only when remote ports are set to **receive off** or **receive desired**.

Cisco uBR10012 Universal Broadband Router

Flow control is supported only on the 1-Port 10-Gigabit Ethernet SPA installed on a Cisco ubR10012 router.

Examples

The following example sets hardware flow control on line 7:

```
line 7
 flowcontrol hardware
```

Catalyst 6500 Series Switches and Cisco 7600 Series Routers

These examples show how to configure the local port to not support any level of flow control by the remote port:

```
Router(config-if)# flowcontrol receive off
Router(config-if)#

Router(config-if)# flowcontrol send off
Router(config-if)#
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to disable flow control on the Cisco 1-Port 10-Gigabit Ethernet SPA:

```
Router# configure terminal
Router(config)#interface TenGigabitEthernet1/0/0
Router(config-if)#flowcontrol receive off
```

Related Commands

Command	Description
start-character	Sets the flow control start character.
stop-character	Sets the flow control stop character.
Catalyst 6500 Series Switches and Cisco 7600 Series Routers	
show interfaces flow-control	Displays flow-control information.

gvrp global

To enable Generic VLAN Registration Protocol (GVRP) globally on a device and on an interface, use the **gvrp global** command in global configuration mode. To disable GRVP, use the **no** form of this command.

gvrp global

no gvrp

Syntax Description

This command has no arguments or keywords.

Command Default

GVRP is administratively disabled.

GRVP is administratively enabled on each interface.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

GVRP is operational on an interface only if GVRP is administratively enabled globally at the device level and at the interface level.

When GVRP is operational on an interface, GVRP protocol data units (PDUs) are transmitted out the interface which must be a forwarding IEEE 802.1Q trunk port.

Examples

The following example configures global GVRP on the device and interfaces:

```
Router(config)# gvrp global
```

Related Commands

Command	Description
clear gvrp statistics	Clears GVRP related statistics recorded on one or all GVRP enabled ports.
debug gvrp	Displays GVRP debugging information.
gvrp mac-learning auto	Enables GVRP to provision MAC address learning.
gvrp registration	Sets the registrars in a GID instance associated with an interface.
gvrp timer	Sets period timers that are used in GARP on a given interface.
gvrp vlan create	Enables a GVRP dynamic VLAN.
show gvrp summary	Displays the GVRP configuration at the device level.
show gvrp interface	Displays details of the administrative and operational GVRP states of all or one particular IEEE 802.1Q trunk port in the device.

gvrp mac-learning auto

To disable MAC learning, use the **gvrp mac-learning** command in global configuration mode. To enable learning of dynamic mac-entries, use the **no** form of this command.

gvrp mac-learning auto

no gvrp mac-learning auto

Syntax Description

This command has no arguments or keywords.

Command Default

MAC learning is enabled by default.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Disables MAC learning on VLANs that are configured with Compact Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) (cGVRP).

Examples

The following example disables MAC learning:

```
Router(config)# gvrp mac-learning auto
```

Related Commands

Command	Description
clear gvrp statistics	Clears GVRP-related statistics recorded on one or all GVRP enabled ports.
debug gvrp	Displays GVRP debugging information.
gvrp global	Enables GVRP globally on a device and on a particular interface.
gvrp registration	Sets the registrars in a GID instance associated with an interface.
gvrp timer	Sets period timers that are used in GARP on a given interface.
gvrp vlan create	Enables a GVRP dynamic VLAN.
show gvrp summary	Displays the GVRP configuration at the device level.
show gvrp interface	Displays details of the administrative and operational GVRP states of all or one particular.1Q trunk port in the device.

gvrp registration

To set the registrars in a global information distribution (GID) instance associated with an interface, use the **gvrp registration** command in global configuration mode. To disable the registrars, use the **no** form of this command.

gvrp registration {**normal** | **fixed** | **forbidden**}

no gvrp registration

Syntax Description

normal	Registrar responds normally to incoming GVRP messages.
fixed	Registrar ignores all incoming GVRP messages and remains in the IN state.
forbidden	Registrar ignores all incoming GVRP messages and remains in the EMPTY (MT) state.

Command Default

Normal

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **gvrp registration** command is only operational if GVRP is configured on an interface.

The **no gvrp registration** command sets the registrar state to the default.

The maximum number of Registrars is 4094.

Examples

The following example sets a fixed, forbidden, and normal registrar on a GID instance:

```
gvrp global
!
int g6/1
gvrp registration fixed
!
int g6/2
gvrp registration forbidden
!
int g6/3
no gvrp registration
```

Related Commands

Command	Description
clear gvrp statistics	Clears GVRP related statistics recorded on one or all GVRP enabled ports.
debug gvrp	Displays GVRP debugging information.
gvrp global	Enables GVRP globally on a device and on a particular interface.
gvrp mac-learning auto	Disables MAC learning.
gvrp timer	Sets period timers that are used in GARP on a given interface.
gvrp vlan create	Enables a GVRP dynamic VLAN.
show gvrp summary	Displays the GVRP configuration at the device level.
show gvrp interface	Displays details of the administrative and operational GVRP states of all or one particular.1Q trunk port in the device.

gvrp timer

To set period timers that are used in General Attribute Registration Protocol (GARP) on an interface, use the **gvrp timer** command in interface configuration mode. To remove the timer value, use the **no** form of this command.

gvrp timer {**join** | **leave** | **leave-all**} *timer-value*

no gvrp timer {**join** | **leave** | **leave-all**}

Syntax Description

join	Time interval between two transmit PDUs.
leave	Time before a Registrar is moved to MT from LV.
leave-all	Time it takes for a LeaveAll timer to expire.
timer-value	Value in milliseconds for the associated keyword. Valid entries are as follows: • Join timer value range is 200 to 100000000 • Leave timer value range is 600 to 100000000 • LeaveAll timer value range is 10000 to 100000000

Command Default

Join timer value default is 200 milliseconds.

Leave timer value default is 600 milliseconds.

LeaveAll time value default is 10000 milliseconds.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **no gvrp timer** command resets the timer value to the default value.

Examples

The following example sets timer levels on an interface:

```
gvrp global
!
int g6/1
!
gvrp timer join 1000
!
gvrp timer leave 1200
!
no gvrp timer leaveall
```

Related Commands

Command	Description
clear gvrp statistics	Clears GVRP related statistics recorded on one or all GVRP enabled ports.
debug gvrp	Displays GVRP debugging information.
gvrp global	Enables GVRP globally on a device and on a particular interface.
gvrp mac-learning auto	Disables MAC learning.
gvrp registration	Sets the registrars in a GID instance associated with an interface.
gvrp vlan create	Enables a GVRP dynamic VLAN.
show gvrp summary	Displays the GVRP configuration at the device level.
show gvrp interface	Displays details of the administrative and operational GVRP states of all or one particular.1Q trunk port in the device.

gvrp vlan create

To enable a Generic VLAN Registration Protocol (GVRP) on a device, use the **gvrp vlan create** command in global configuration mode. To disable a dynamic VLAN, use the **no** form of this command.

gvrp vlan create

no gvrp vlan create

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

VLAN Trunk Protocol (VTP) must be in transparent mode in order to configure a GVRP dynamic VLAN.

Examples

The following example configures a GVRP dynamic VLAN:

```
vtp mode transparent
!
gvrp vlan create
```

Related Commands

Command	Description
clear gvrp statistics	Clears GVRP related statistics recorded on one or all GVRP enabled ports.
debug gvrp	Displays GVRP debugging information.
gvrp global	Enables GVRP globally on a device and on a particular interface.
gvrp mac-learning auto	Enables a GRVP dynamic VLAN on a device.
gvrp registration	Sets the registrars in a GID instance associated with an interface.
gvrp timer	Sets period timers that are used in GARP on a given interface.
show gvrp summary	Displays the GVRP configuration at the device level.
show gvrp interface	Displays details of the administrative and operational GVRP states of all or one particular.1Q trunk port in the device.

hw-module slot (ASR 1000 Series)

To start, stop, reload, or enable logging for an Embedded Services Processor (ESP), Route Processor (RP), or Shared Port Adapter (SPA) Interface Processor (SIP) on a Cisco ASR 1000 Series Aggregation Services Router, use the **hw-module slot** command in privileged EXEC or global configuration or diagnostic mode.

hw-module slot *slot action*

Syntax Description

slot	Slot on which logging action is to be taken. Options are as follows: • *number*—the number of the SIP slot. • **f0**—The ESP in ESP slot 0. • **f1**—The ESP in ESP slot 1 • **r0**—The RP in RP slot 0. • **r1**—The RP in RP slot 1.
action	The action to take on the hardware in the specified *slot*. Options are as follows: • **logging onboard** [**disable** | **enable**]—Disables or enables onboard logging of the hardware. • **reload**—Reloads the specified hardware. • **start**—Starts the hardware if it has been stopped. • **stop**—Stops the hardware if it is currently active.

Command Default

The router sends and receives traffic by default, so this command is not necessary to enable any hardware on a router.
Onboard logging for all of the hardware is enabled by default.

Command Modes

Diagnostic (diag)
Privileged EXEC (#)
Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

The **hw-module slot** command does not have a **no** form.

To start, stop, or reload a SPA, use the **hw-module subslot** command.

The **stop** and **reload** options cannot be used on an active RP.

All traffic to hardware that has been set to stop using the **stop** option will be dropped until the hardware is reenabled by either physically removing and reinserting the hardware, or entering the **start** option. After the hardware is modified as appropriate or the **start** option is entered, the hardware has to reinitialize before it is able to send and receive traffic. Note that in some cases reinitialization can take several minutes, and that the reinitialization time required depends on the hardware and the system configuration.

When a SIP is stopped, all traffic to all SPAs in the SIP is dropped. The SPAs in the SIP can begin receiving traffic after the SIP is restarted using the **start** option and all SPAs and the SIP finish reinitializing.

Since this is a privileged EXEC-level command, this command setting cannot be saved to the startup configuration and therefore the command setting cannot be maintained after a system reload. If you want the hardware to stay in the **stop** state across system reloads, use the **hw-module slot** *slot* **shutdown** global configuration command.

The **reload** option can be used to reload hardware for any reason; for example, to finish a software upgrade that requires reloading of the hardware or to reload the hardware as part of a troubleshooting step.

The contents of onboard logging logs can be displayed using the **show logging onboard slot** privileged EXEC and diagnostic mode commands.

Enter the **show logging onboard slot** *slot* **status** privileged EXEC or diagnostic command to see if onboard logging is enabled or disabled for the hardware in a particular slot.

When the **hw-module slot** *slot* **logging onboard disable** command is entered, onboard logging for the specified hardware component is disabled but the existing logs are preserved; if you want to erase the existing logs, enter the **clear logging onboard slot** command.

When the **hw-module slot** command is entered in global configuration mode (for ESP40 and SIP40 cards), you have a link option that allows you to choose among a set of backplane enhanced serializer/deserializer (SerDes) interconnect (ESI) links between ESP and a given SIP slot. The range of possible values for the link depends on the type of ESP and SIP cards. Only a combination of ESP40 and SIP40 cards can have more than two ESI links (link A and link B). All other cards have only link A. For example, a combination of ESP40 and SIP10 or ESP20 and SIP40 cards can have only one link (link A).

Examples

The following example shows how to stop the RP in RP slot 0:

```
Router# hw-module slot r0 stop
```

The following example shows how to disable the onboard logging for the RP in RP slot 0. The output of the **show logging onboard slot r0 status** command is given both before and after onboard logging is disabled to verify that onboard logging was properly disabled.

```
Router# show logging onboard slot r0 status

Status: Enabled

Router# hw-module slot r0 logging onboard disable

Router# show logging onboard slot r0 status

Status: Disabled
```

The following example shows how to display the available link options for ESP40 and SIP40 cards:

```
Router(config)# hw-module slot 0 qos input link ?
A  ESI Link A
B  ESI Link B
```

Related Commands

Command	Description
clear logging onboard slot	Clears the data in an onboard slot log.
hw-module subslot	Starts, stops, or reloads a SPA.
show logging onboard slot	Displays the status of onboard logging, or the contents of an onboard logging log.

instance (VLAN)

To map a VLAN or a group of VLANs to a multiple spanning tree (MST) instance, use the **instance** command in MST configuration mode. To return the VLANs to the default command and internal spanning tree (CIST), use the **no** form of this command.

instance *instance-id* **vlans** *vlan-range*

no instance *instance-id*

Syntax Description

instance-id	Instance to which the specified VLANs are mapped; valid values are from 0 to 4094.
vlans *vlan-range*	Specifies the number of the VLANs to be mapped to the specified instance; valid values are from 1 to 4094.

Defaults

No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).

Command Modes

MST configuration mode (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 Cisco IOS Release 12.2 (17d)SXB.
12.2(18)SXF	This command was changed as follows: • You can configure up to 65 interfaces. • You can designate the *instance-id* from 1 to 4094.

Usage Guidelines

The **vlans** *vlan-range* is entered as a single value or a range.

The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added or removed to the existing instances.

Any unmapped VLAN is mapped to the CIST instance.

Examples

The following example shows how to map a range of VLANs to instance 2:

```
Router(config-mst)# instance 2 vlans 1-100
Router(config-mst)#
```

The following example shows how to map a VLAN to instance 5:

```
Router(config-mst)# instance 5 vlans 1100
Router(config-mst)#
```

The following example shows how to move a range of VLANs from instance 2 to the CIST instance:

```
Router(config-mst)# no instance 2 vlans 40-60
Router(config-mst)#
```

The following example shows how to move all the VLANs that are mapped to instance 2 back to the CIST instance:

```
Router(config-mst)# no instance 2
Router(config-mst)#
```

Related Commands

Command	Description
name (MST configuration mode)	Sets the name of an MST region.
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 mist configuration	Enters MST configuration mode.

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 **mac access-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.

Defaults

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 **mac access-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 **mac access-list extended** 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**.

Usage Guidelines

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 **mac access-list extended** *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).

For the Cisco 7600 series platform when ES20 or ES40 line cards are used, only the {**permit** | **deny**} {*src-mac mask* | **any**} {*dest-mac mask* | **any**} part of the command syntax applies. If an extended MAC Access Control List is created using the [**protocol** [**vlan** *vlan*] [**cos** *value*]] options, these options are ignored.

Table 1 describes the syntax of the **mac access-list extended** 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-address source-mac-address-mask*.
any	Specifies any protocol type.
dest-mac mask	(Optional) Destination MAC address in the form: *dest-mac-address dest-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.
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**—LACP encapsulated packets
- **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-mac mask* or *dest-mac mask* 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 **deny any any** entry exists at the end of an access list unless you include an explicit **permit any any** 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 **mac access-list extended** 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-table aging-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.
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.

Release	Modification
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

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

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

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

Catalyst Switches and Cisco 7600 Routers

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

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

Catalyst Switches

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

no mac-address-table dynamic *hw-address* [**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.

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

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-table aging-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-table static	Adds static addresses to the MAC address table.
show mac-address-table	Displays the MAC address table.

mac-address-table learning

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

[**default**] **mac-address-table learning** {**vlan** *vlan-id* | **interface** *interface slot*/*port*} [**module** *num*]

no mac-address-table learning {**vlan** *vlan-id* | **interface** *interface slot*/*port*} [**module** *num*]

Syntax Description

default	(Optional) Returns to the default settings.
vlan *vlan-id*	Specifies the VLAN to apply the per-VLAN learning of all MAC addresses; valid values are from 1 to 4094.
interface	Specifies per-interface based learning of all MAC addresses.
interface slot/*port*	Interface type, the slot number, and the port number.
module *num*	(Optional) Specifies the module number.

Defaults

If you configure a VLAN on a port in a module, all the supervisor engines and Distributed Forwarding Cards (DFCs) in the Catalyst 6500 series switch are enabled to learn all the MAC addresses on the specified VLAN.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	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

You can use the **module** *num* keyword and argument to specify supervisor engines or DFCs only.

You can use the **vlan** *vlan-id* keyword and argument on switch-port VLANs only. You cannot use the **vlan** *vlan-id* keyword and argument to configure learning on routed interfaces.

You can use the **interface** *interface slot*/*port* keyword and arguments on routed interfaces, supervisor engines, and DFCs only. You cannot use the **interface** *interface slot*/*port* keyword and arguments to configure learning on switch-port interfaces or non-DFC modules.

Examples

This example shows how to enable MAC-address learning on a switch-port interface on all modules:

```
Router(config)# mac-address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC-address learning on a switch-port interface on a specified module:

```
Router(config)# mac-address-table learning vlan 100 module 4
Router(config)#
```

This example shows how to disable MAC-address learning on a specified switch-port interface for all modules:

```
Router(config)# no mac-address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC-address learning on a routed interface on all modules:

```
Router(config)# mac-address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC-address learning on a routed interface for a specific module:

```
Router(config)# mac-address-table learning interface FastEthernet 3/48 module 4
Router(config)#
```

This example shows how to disable MAC-address learning for all modules on a specific routed interface:

```
Router(config)# no mac-address-table learning interface FastEthernet 3/48
Router(config)#
```

Related Commands

Command	Description
show mac-address-table learning	Displays the MAC-address learning state.

mac-address-table limit

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

mac-address-table limit [**action** {**warning** | **limit** | **shutdown**}] [**notification** {**syslog** | **trap** | **both**}] [**interface** *type mod/port*] [**maximum** *num*] [**vlan** *vlan*] [**maximum** *num*] [**action** {**warning** | **limit** | **shutdown**}] [**flood**]

no mac-address-table limit [**action** {**warning** | **limit** | **shutdown**}] [**notification** {**syslog** | **trap** | **both**}] [**interface** *type mod/port*] [**maximum** *num*] [**vlan** *vlan*] [**maximum** *num*] [**action** {**warning** | **limit** | **shutdown**}] [**flood**]

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.

Defaults

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** *type mod/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** *type mod/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-table limit** 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-table limit** 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-table notification change** 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:
  - **histor**y *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.
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-table notification mac-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 notification threshold

To enable content-addressable memory (CAM) table usage monitoring notification, use the **mac-address-table notification threshold** command in global configuration mode. To disable CAM table usage monitoring notification, use the **no** form of this command.

mac-address-table notification threshold limit *percentage* **interval** *seconds*

no mac-address-table notification threshold

Syntax Description

limit *percentage*	Specifies the percentage of the CAM utilization; valid values are from 1 to 100 percent.
interval *seconds*	Specifies the time in seconds between notifications; valid values are greater than or equal to 120 seconds.

Defaults

The defaults are as follows:

- Disabled.
- *percentage* is **50** percent.
- *seconds* is **120** seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	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

When you enable CAM table usage monitoring, the number of valid entries in the CAM table are counted and if the percentage of the CAM utilization is higher or equal to the specified threshold, a message is displayed.

Examples

This example shows how to enable CAM table usage monitoring notification and use the default settings:

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

This example shows how to enable CAM table usage monitoring notification and set the threshold and interval:

```
Router(config)# mac-address-table notification threshold limit 20 interval 200
Router(config)#
```

This example shows how to disable CAM table usage monitoring notification:

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

Related Commands

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

mac-address-table secure

To add secure addresses to the MAC address table, use the **mac-address-table secure** 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

mac-address-table secure *hw-address interface* {**fa** | **gi**} *slot*/*port* **vlan** *vlan-id*

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

Catalyst Switches

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

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

Cisco 860 Series Integrated Services Routers (ISRs) and Cisco 880 Series ISRs

mac-address-table secure [H.H.H | maximum *maximum addresses***]**

no mac-address-table secure [H.H.H | maximum *maximum addresses***]**

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.
H.H.H	(Optional) Specifies 48-bit hardware address.
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.
maximum *maximum addresses*	(Optional) Applies only to Cisco 860 series and Cisco 880 series ISRs. Range is 1–200.

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.
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.
12.4(20)T	This command with the **H.H.H** and **maximum** keyword was added for Cisco Series 860 ISRs and Cisco Series 880 ISRs.

Usage Guidelines

Cisco 860 Series ISRs, Cisco 880 Series ISRs, Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

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.

If the maximum number is more than the MAC addresses statically specified by using the **H.H.H** keyword, the switch learns the MAC address automatically up to the specified maximum. If the maximum number is less than the number of MAC addresses already specified statically, then an error message displays.

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

Cisco 860 Series ISRs, Cisco 880 Series ISRs

The following example shows how to allow ten devices on Fast Ethernet port 2:

```
Router(config)# mac-address-table secure maximum 10 ?
FastEthernet  FastEthernet IEEE 802.3

Router(config)# mac-address-table secure maximum 10 f ?
<0-4>  FastEthernet interface number

Router(config)# mac-address-table secure maximum 10 f 2
```

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

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
```

Catalyst Switches

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-table aging-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-table dynamic	Adds dynamic addresses to the MAC address table.
mac-address-table static	Adds static addresses to the MAC address table.
show mac-address-table	Displays the MAC address table.

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, and Cisco 3700 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** *int* | **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** *int* | **drop** [**disable-snooping**]} [**dlci** *dlci* | **pvc** *vpi/vci*] [**auto-learn** | **disable-snooping**] [**protocol** {**ip** | **ipx** | **assigned**}]

Syntax Description

mac-address	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** *int*	Specifies the interface type and the slot and port to be configured. On the Catalyst switches, the *int* argument 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. The valid range is from 16 to 1007. **Note** This option is valid 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 valid 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 changed to support multicast addresses.
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.
12.2(17a)SX	You cannot apply the **mac-address-table static** *mac-addr* **vlan** *vlan-id* **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	The **dlci** and **pvc** options were added to allow mapping a MAC address to a Frame Relay data-link connection identifier (DLCI) or ATM permanent virtual circuit (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 output interface specified cannot be a switched virtual interface (SVI).

Entering 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 output interface specified 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*, 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 output interface specified must be a Layer 2 IDB and not an SVI.

The **ipx** keyword is not supported.

You can enter up to 15 interfaces per command entered, but 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** *int* 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.

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

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.

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

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

```
Router(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 always using the **dlci** and **pvc** keywords on the appropriate interfaces.

Examples

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

```
Router(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:

```
Router(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:

```
Router(config)# mac-address-table static 0C01.0203.0405 vlan 101 interface ATM6/1 pvc
6/101
Router(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 synchronize

To synchronize the Layer 2 MAC address table entries across the Policy Feature Card (PFC) and all the Distributed Forwarding Cards (DFCs), use the **mac-address-table synchronize** command in global configuration mode. To disable MAC address table synchronization or reset the activity timer, use the no form of this command.

mac-address-table synchronize [**activity-time** *seconds*]

no mac-address-table synchronize [**activity-time** *seconds*]

Syntax Description

activity-time *seconds*	(Optional) Specifies the activity timer interval: valid values are 160, 320, and 640 seconds.

Defaults

The default settings are as follows:

- Layer 2 MAC address table entries are not synchronized by default.
- Enabled for WS-X6708-10GE.
- If the command is enabled, the value of the **activity-time** keyword is 160 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(18)SXF5	The default for this command was changed to enabled for the WS-X6708-10GE.
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 updated.

Usage Guidelines

We recommend that you configure the activity time so that at least two activity times exist within the regular Layer 2 aging time (or within the aging time used for VLANs in distributed EtherChannels if this feature is used only for distributed EtherChannels). If at least two activity times do not exist within the aging time, then an error message is displayed.

Examples

This example shows how to specify the activity timer interval :

```
Router(config)# mac-address-table synchronization activity time 160
Router(config)#
```

This example shows how to specify the activity timer interval when Out-of-Band (OOB) synchronization is enabled:

```
Router(config)# mac-address-table synchronization activity time 160
 % Current OOB activity time is [160] seconds
 % Recommended aging time for all vlans is atleast three times the activity interval and
 global aging time will be changed automatically if required
Router(config)#
```

This example shows how to display the timer interval:

```
Router(config)# mac-address-table synchronization
Router(config)#
```

This example shows how to display the timer interval when OOB synchronization is enabled:

```
Router(config)# mac-address-table synchronization
 % Current OOB activity time is [160] seconds
 % Recommended aging time for all vlans is atleast three times the activity interval
Router(config)#
```

Related Commands

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

mac-address-table unicast-flood

To enable unicast-flood protection, use the **mac-address-table unicast-flood** command in global configuration mode. To disable unicast-flood protection, use the **no** form of this command.

mac-address-table unicast-flood limit *kfps* **vlan** *vlan-id* {**filter** *minutes* | **alert** | **shutdown**}

no mac-address-table unicast-flood limit *kfps* **vlan** *vlan*

Syntax Description

limit *kfps*	Limits the unicast floods on a per-source MAC address and per-VLAN basis; valid values are from 1 to 4000 thousand floods per second (Kfps).
vlan *vlan-id*	Specifies the VLAN to apply the flood limit; valid values are from 1 to 4094.
filter *minutes*	Specifies how long in minutes to filter unicast floods; valid values are from 1 to 34560 minutes.
alert	Specifies when frames of unicast floods exceed the flood rate limit to send an alert.
shutdown	Specifies when frames of unicast floods exceed the flood rate limit to shut down the ingress port generating the floods.

Defaults

Unicast-flood protection is not enabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

We recommend that you configure unicast-flood protection as follows:

- Set the **limit** *kfps* argument to 10 Kfps.
- Set the **filter** *minutes* argument to 5 minutes.

The **shutdown** keyword is supported on nontrunk ports only.

If you specify **alert** and unknown unicast floods exceeding the threshold are detected, a system message is displayed and no further action is taken.

If you specify **shutdown** and unknown unicast floods exceeding the threshold are detected, a system message is displayed. Once the system message is displayed, the port goes to err-disable mode.

Examples

This example shows how to set the flood rate limit to 3000 floods per second (fps) and display a system message when the rate limit has been exceeded:

```
Router(config)# mac-address-table unicast-flood limit 3 vlan 125 alert
Router(config)#
```

Related Commands

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

match (VLAN access-map)

To specify the match clause by selecting one or more IP, Internetwork Packet Exchange (IPX), or MAC access control lists (ACLs) for a VLAN access-map sequence for traffic filtering, use the **match** command in VLAN access-map configuration mode. To remove the match clause, use the **no** form of this command.

match {**ip address** {*acl-number* | *acl-name*} | **ipx address** {*acl-number* | *acl-name*} | **mac address** *acl-name*}

no match {**ip address** {*acl-number* | *acl-name*} | **ipx address** {*acl-number* | *acl-name*} | **mac address** *acl-name*}

Syntax Description

ip address *acl-number*	Selects one or more IP ACLs for a VLAN access-map sequence; valid values are from 1 to 199 and from 1300 to 2699.
ip address *acl-name*	Selects an IP ACL by name.
ipx address *acl-number*	Selects one or more IPX ACLs for a VLAN access-map sequence; valid values are from 800 to 999.
ipx address *acl-name*	Selects an IPX ACL by name.
mac address *acl-name*	Selects one or more MAC ACLs for a VLAN access-map sequence.

Defaults

No match clause is specified.

Command Modes

VLAN access-map configuration (config-access-map)

Command History

Release	Modification
12.1(8a)E3	This command was introduced on the Cisco 7600 series routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **match ipx address** and **match mac address** commands are not supported for VLAN ACLs (VACLs) on WAN interfaces.

IPX ACLs that are used in VACLs can specify only the IPX protocol type, the source network, the destination network, and the destination host address.

The MAC sequence is not effective for IP or IPX packets. IP packets and IPX packets should be access controlled by IP and IPX match clauses.

You cannot configure VACLs on secondary VLANs. The secondary VLAN inherits all features that are configured on the primary VLAN.

The following commands appear in the command-line interface (CLI) help but are not supported by the quality of service (QoS) as implemented on the policy feature card (PFC):

- **match any**
- **match class-map**
- **match cos**
- **match destination-address mac**
- **match input-interface**
- **match mpls experimental**
- **match mpls experimental topmost**
- **match mpls-label**
- **match qos-group**
- **match source-address mac**

Examples

The following example defines a match clause for a VLAN access map:

```
Router(config)# vlan access-map map1 10
Router(config-access-map)# match ip address 13
```

Related Commands

Command	Description
action	Sets the packet action clause.
match any	Configures the match criteria for a class map to be successful match criteria for all packets.
match class-map	Configures a traffic class as a classification policy.
match cos	Configures the device to match a packet based on a Layer 2 CoS marking.
match destination-address mac	Configures the destination MAC address as a match criterion.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified value of the EXP field as a match criterion.
match mpls experimental topmost	Configures a class map to use the EXP value in the topmost label as a match criterion.
match mpls-label	Redistributes routes that include MPLS labels if the routes meet the conditions specified in the route map.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
match qos-group	Configures a specific QoS group value as a match criterion.
match source-address mac	Configures the source MAC address as a match criterion.
port access-map	Creates a port access map or enters port access-map command mode.

Command	Description
show vlan access-map	Displays the contents of a VLAN access map.
vlan access-map	Creates a VLAN access map or enters VLAN access-map configuration mode.

mls rp ip

To enable the Multilayer Switching Protocol (MLSP) and multilayer switching (MLS), use the **mls rp ip** command in global configuration mode. To disable MLS, use the **no** form of this command.

mls rp ip

no mls rp ip

Syntax Description

This command has no arguments or keywords.

Command Default

MLS is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(3) WA4(4)	This command was introduced.
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

Use this command to enable MLS, either globally or on a specific interface. MLSP is the protocol that runs between the switches and routers.

Examples

The following example enables MLS:

```
Router(config)# mls rp ip
```

Related Commands

Command	Description
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp nde-address	Specifies a NetFlow Data Export address.
mls rp vlan-id	Assigns a VLAN ID.
mls rp vtp-domain	Selects the router interface to be Layer 3 switched and then adds that interface to a Virtual Trunking Protocol (VTP) domain.
show mls rp	Displays MLS details, including specifics for MLSP.
show mls rp vtp-domain	Displays MLS interfaces for a specific VTP domain.

mls rp ip (global)

To enable external systems to establish IP shortcuts to the Multilayer Switching Feature Card (MSFC), use the **mls rp ip** command in global configuration mode. To remove a prior entry, use the **no** form of this command.

mls rp ip [**input-acl** | **route-map**]

no mls rp ip

Syntax Description

input-acl	(Optional) Enables the IP-input access list.
route-map	(Optional) Enables the IP-route map.

Defaults

No shortcuts are configured.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to allow the external systems to establish IP shortcuts with IP-input access lists:

```
Router(config)# mls rp ip input-acl
Router(config)#
```

Related Commands

Command	Description
mls ip	Enables MLS IP for the internal router on the interface.
show mls ip multicast	Displays the MLS IP information.

mls rp ip (interface)

To enable the external systems to enable Multilayer Switching (MLS) IP on a specified interface, use the **mls rp ip** command in interface configuration mode. To disable MLS IP, use the **no** form of this command.

mls rp ip

no mls rp ip

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

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(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.

Examples

This example shows how to enable the external systems to enable MLS IP on an interface:

```
Router(config-if)# mls rp ip
Router(config-if)
```

Related Commands

Command	Description
mls rp ip (global)	Enables external systems to establish IP shortcuts to the MSFC.
show mls ip multicast	Displays the MLS IP information.

mls rp ip multicast

To enable IP multicast multilayer switching (MLS) (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch, use the **mls rp ip multicast** command in interface configuration mode. To disable IP multicast MLS on the interface or VLAN, use the **no** form of this command.

mls rp ip multicast

no mls rp ip multicast

Syntax Description

This command has no arguments or keywords.

Command Default

IP multicast MLS is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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

This command is available only on specific router platforms connected to a Catalyst 5000 switch. Use this command to reduce multicast load on the router. The switch performs the multicast packet replication and forwarding.

IP multicast MLS is enabled by default on an interface after IP multicast routing and Protocol Independent Multicast (PIM) are enabled.

Examples

The following example shows how to disable IP multicast MLS:

```
Router(config)# interface fastethernet1/0.1
Router(config-if)# no mls rp ip multicast
```

Related Commands

Command	Description
mls rp ip multicast management-interface	Assigns a different interface (other than the default) to act as the management interface for MLSP.
show ip mroute	Displays the contents of the IP multicast routing table.
show mls rp interface	Displays hardware-switched multicast flow information about IP multicast MLS.

mls rp ip multicast management-interface

To assign a different interface (other than the default) to act as the management interface for Multilayer Switching (MLS), use the **mls rp ip multicast management-interface** command in interface configuration mode. To restore the default interface as the management interface, use the **no** form of this command.

mls rp ip multicast management-interface

no mls rp ip multicast management-interface

Syntax Description

This command has no arguments or keywords.

Command Default

When IP multicast MLS is enabled, the subinterface (or VLAN interface) that has the lowest VLAN ID and is active (in the "up" state) is automatically selected as the management interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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

When you enable IP multicast MLS, the subinterface (or VLAN interface) that has the lowest VLAN ID and is active (in the "up" state) is automatically selected as the *management interface*. The one-hop protocol Multilayer Switching Protocol (MLSP) is used between a router and a switch to pass messages about hardware-switched flows. MLSP packets are sent and received on the management interface. Typically, the interface in VLAN 1 is chosen (if that interface exists). Only one management interface is allowed on a single trunk link.

In most cases, we recommend that the management interface be determined by default. However, you can optionally use this command to specify a different router interface or subinterface as the management interface. We recommend using a subinterface with minimal data traffic so that multicast MLSP packets can be sent and received more quickly.

If the user-configured management interface goes down, the router uses the default interface (the active interface with the lowest VLAN ID) until the user-configured interface comes up again.

Examples

The following example shows how to configure the Fast Ethernet interface as the management interface:

```
Router(config)# interface fastethernet1/0.1
Router(config-if)# mls rp ip multicast management-interface
```

Related Commands

Command	Description
mls rp ip multicast	Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.

mls rp ipx (global)

To enable the router as a multilayer switching (MLS) IPX Route Processor (RP), or to allow the external systems to enable MLS IPX to a Multilayer Switch Feature Card (MSFC), use the **mls rp ipx** command in global configuration mode. To disable MLS IPX on the router or MSFC, use the **no** form of this command.

mls rp ipx [**input-acl**]

no mls rp ipx [**input-acl**]

Syntax Description

input-acl	(Optional for Cisco 7600 series only) Enables MLS IPX and overrides ACLs.

Command Default

MLS IPX is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(17d)SXB	This command was integrated into Cisco IOS 12.2(17d)SXB and introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Multilayer Switching Protocol (MLSP) is the protocol that runs between the MLS switching engine and the MLS RP.

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

Examples

The following example enables MLS IPX on the MLS RP:

```
Router(config)# mls rp ipx
```

This example shows how to allow the external systems to enable MLS IPX to the MSFC and override ACLs:

```
Router(config)# mls rp ipx input-acl
Router(config)#
```

Related Commands

Command	Description
mls rp ipx (interface)	Enables MLS IPX on a router interface.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an MLS IPX interface.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays MLS IPX details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all MLS IPX interfaces on the MLS IPX router.
show mls rp vtp-domain	Displays MLS IPX interfaces for a specific VTP domain on the RP.

mls rp ipx (interface)

To enable multilayer switching (MLS) Internetwork Packet Exchange (IPX) on a router interface, use the **mls rp ipx** command in interface configuration mode. To disable MLS IPX on a router interface, use the **no** form of this command.

mls rp ipx

no mls rp ipx

Syntax Description

This command has no arguments or keywords.

Command Default

MLS IPX is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(17d)SXB	This command was integrated into Cisco IOS 12.2(17d)SXB and introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Multilayer Switching Protocol (MLSP) is the protocol that runs between the MLS Switching Engine and the MLS RP.

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

Examples

The following example shows how to enable MLS IPX on a router interface:

```
Router(config-if)# mls rp ipx
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an MLS IPX RP, or allows the external systems to enable MLS IPX to an MSFC.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an MLS IPX interface.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays MLS IPX details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all MLS IPX interfaces on the MLS IPX router.
show mls rp vtp-domain	Displays MLS IPX interfaces for a specific VTP domain on the RP.

mls rp locate ipx

To display information about all switches currently shortcutting for the specified Internetwork Packet Exchange (IPX) flows, use the **mls rp locate ipx** command in privileged EXEC mode.

mls rp locate ipx *destination-network.destination-node* [*source-network*]

Syntax Description

destination-network.destination-node	The destination network and destination node of IPX packet flows. The destination network address consists of 1 to 8 hexadecimal numbers in the format xxxxxxxx. The destination node address consists of 12 hexadecimal numbers in the format xxxx.xxxx.xxxx.
source-network	(Optional) The source network of the IPX flow. The address of the source network consists of 1 to 8 hexadecimal numbers in the format yyyyyyyy.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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.

Examples

The following example shows how to display the switch that is shortcutting routed flows to the specified IPX flow:

```
Router# mls rp locate ipx 30.0000.1111.2222

    locator response from switch id 0010.1400.601f
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp management-interface

To specify an interface as the management interface, use the **mls rp management-interface** command in interface configuration mode. To remove an interface as the management interface, use the **no** form of this command.

mls rp management-interface

no mls rp management-interface

Syntax Description

This command has no keywords or arguments.

Command Default

No interface is specified as the management interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(3)WA4(4)	This command was introduced.
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)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Multilayer Switching Protocol (MLSP) packets are sent and received through the management interface.

Select only one IPX multilayer switching (MLS) interface connected to the switch. If you fail to select this interface, no connection between the MLS route processor (RP) and the MLS switching engine occurs, and any routing updates or changes to access lists are not reflected on the switch.

Examples

The following example shows how to select a management interface:

```
Router(config-if)# mls rp management-interface
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp nde-address

To specify a NetFlow Data Export (NDE) address, use the **mls rp nde-address** command in global configuration mode. To remove the NDE address, use the **no** form of this command.

mls rp nde-address [*ip-addr*]

no mls rp nde-address [*ip-addr*]

Syntax Description

ip-address	(Optional) NDE IP address.

Command Default

No NDE address is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(3)WA4(4)	This command was introduced.
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(17d)SXB release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command on a route processor (RP) to specify the NDE address for a router. If you *do not* specify an NDE IP address for the multilayer switching (MLS) RP, the MLS RP automatically selects one of its interface's IP addresses and uses that IP address as its NDE IP address *and* its MLS IP address.

Use the following syntax to specify an IP subnet address:

- *ip-subnet-addr*—Short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP-subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 172.24.00.00 indicates a 16-bit subnet address (subnet mask 172.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.
- *ip-addr/subnet-mask*—Long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip-addr* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip-addr/maskbits*—Simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip-addr* is a full host address, such as 192.168.253.1/22, which has the same subnet address as the *ip-subnet-addr*.

Examples

The following example shows how to set the NDE address to 172.25.2.1:

```
Router(config)# mls rp nde-address 172.25.2.1
```

Related Commands

Command	Description
mls rp ip	Enables MLSP.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN ID.
mls rp vtp-domain	Selects the router interface to be Layer 3 switched and then adds that interface to a VTP domain.
show mls rp	Displays MLS details, including specifics for MLSP.
show mls rp vtp-domain	Displays MLS interfaces for a specific VTP domain.

mls rp vlan-id

To assign a VLAN identification number to an interface, use the **mls rp vlan-id** command in interface configuration mode. To remove a VLAN identification number, use the **no** form of this command.

mls rp vlan-id *vlanid-number*

no mls rp vlan-id *vlanid-number*

Syntax Description

vlanid-number	A VLAN identification number from 1 to 4094.

Command Default

No VLAN identification number is assigned.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(3)WA4(4)	This command was introduced.
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 Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows how to assign the VLAN identification number to an interface:

```
Router(config-if)# mls rp vlan-id 23
```

Related Commands

Command	Description
show mls rp	Displays MLS details.

mls rp vtp-domain

To assign a multilayer switching (MLS) interface to a specific Virtual Trunking Protocol (VTP) domain on the MLS Route Processor (RP), use the **mls rp vtp-domain** command in interface configuration mode. To remove a VTP domain, use the **no** form of this command.

mls rp vtp-domain *domain-name*

no mls rp vtp-domain *domain-name*

Syntax Description

domain-name	The name of the VTP domain assigned to an MLS interface and its related switches.

Command Default

The interface is assigned to the null domain.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(3)WA4(4)	This command was introduced.
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)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The assigned IPX MLS interface must be either an Ethernet interface or a Fast Ethernet interface—both without subinterfaces.

Examples

The following example shows how to assign the MLS interface to the VTP domain named engineering:

```
Router(config-if)# mls rp vtp-domain engineering
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
vtp	Configures the global VTP state.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls switching

To enable the hardware switching, use the **mls switching** command in global configuration mode. To disable hardware switching, use the **no** form of this command.

mls switching

no mls switching

Syntax Description

This command has no arguments or keywords.

Defaults

Hardware switching 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(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:

```
Router(config)# mls switching
Router(config)#
```

This example shows how to disable the hardware switching:

```
Router(config)# no mls switching
Router(config)#
```

Related Commands

Command	Description
mls switching unicast	Enables the hardware switching of the unicast traffic for an interface.

mls switching unicast

To enable the hardware switching of the unicast traffic for an interface, use the **mls switching unicast** 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.

Defaults

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 **mode dot1q-in-dot1q access-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.

Defaults

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 **mode dot1q-in-dot1q access-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 **mode dot1q-in-dot1q access-gateway** command.

After configuring the **mode dot1q-in-dot1q access-gateway** command, use the **bridge-domain (subinterface configuration)** command to configure the VLAN mapping to be used on each subinterface.

Caution Using the **mode dot1q-in-dot1q access-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 **mode dot1q-in-dot1q access-gateway** command.

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

Tip The **mls qos trust** command has no effect on a GE-WAN interface or port-channel group that has been configured with the **mode dot1q-in-dot1q access-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 **mode dot1q-in-dot1q access-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 **mode dot1q-in-dot1q access-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 **mode dot1q-in-dot1q access-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 (subinterface configuration)** 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 **mode dot1q-in-dot1q access-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.
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.

Command	Description
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.

monitor session

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

To start a new Switched Port Analyzer (SPAN) session, add or delete interfaces from an existing SPAN session, or delete a SPAN session, use the **monitor session** command in global configuration mode. To remove one or more source interfaces or destination interfaces from the SPAN session, use the **no** form of this command.

Source Interface

monitor session *session* **source interface** *type/slot/port* [**,** | **-** | **rx** | **tx** | **both**]

no monitor session *session* **source interface** *type/slot/port* [**,** | **-** | **rx** | **tx** | **both**]

Destination Interface

monitor session *session* **destination interface** *type/slot/port* [**,** | **-**]

no monitor session *session* **destination interface** *type/slot/port* [**,** | **-**]

Session

monitor session *session*

no monitor session *session*

Cisco 6500/6000 Catalyst Switches and Cisco 7600 Series Routers

To start a new ERSPAN, SPAN, or RSPAN session, add or delete interfaces or VLANs to or from an existing session, filter ERSPAN, SPAN, or RSPAN traffic to specific VLANs, or delete a session, use the **monitor session** command in global configuration mode. To remove one or more source or destination interfaces from the session, remove a source VLAN from the session, or delete a session, use the **no** form of this command.

Setting the Source Interface or VLAN

monitor session *session* **source** {**interface** *type* | **vlan** *vlan-id* [**rx** | **tx** | **both**] | **remote vlan** *rspan-vlan-id*}

no monitor session *session* **source** {**interface** *type* | **vlan** *vlan-id* [**rx** | **tx** | **both**] | **remote vlan** *rspan-vlan-id*}

Setting the Destination Interface or VLAN

monitor session *session* **destination** {**interface** *type* | **vlan** *vlan-id* | **remote vlan** *vlan-id* | **analysis-module** *slot-number* | {**data-port** *port-number*}

no monitor session *session* **destination** {**interface** *type* | **vlan** *vlan-id* | **remote vlan** *vlan-id* | **analysis-module** *slot-number* | **data-port** *port-number*}

Setting the Filter VLAN

monitor session *session-number* **filter vlan** *vlan-range*

no monitor session *session-number* **filter vlan** *vlan-range*

Setting the Session Type

monitor session *session-number* **type** {**erspan-source | erspan-destination**}

no monitor session {**range** *session-range* **| local | remote | all |** *session*}

Enabling a Service Module

monitor session servicemodule *mod-list*

no monitor session servicemodule *mod-list*

Syntax Description

session-number	Number of the SPAN session. For Cisco 2600, 3600, and 3700 series routers, valid values are 1 and 2. For Cisco 6500/6000 and 7600 series routers, valid values are 1 to 66.
source	Specifies the SPAN source.
destination	Specifies the SPAN destination interface.
interface *type*	(Optional) Specifies the interface type. For the Cisco 2600, 3600, and 3700 series routers, valid values are **fastethernet** and **gigabitethernet**. For the Cisco 6500/6000 and 7600 series routers, valid values are **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**. See the "Usage Guidelines" for formatting information.
slot	(Optional) Specifies the interface number; valid entries are 1 and 2.
port	(Optional) Port interface number ranges 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
interface *type/slot/port*	Specifies the interface type and number; valid values are **ethernet** (1 to 9), **fastethernet** (1 to 9), **gigabitethernet** (1 to 9), and **port-channel** (see the "Usage Guidelines" section).
,	(Optional) Specifies a series of SPAN VLANs.
-	(Optional) Specifies a range of SPAN VLANs.
rx	(Optional) Specifies monitor received traffic only.
tx	(Optional) Specifies monitor transmitted traffic only.
both	(Optional) Specifies monitor received and transmitted traffic.
vlan *vlan-id*	Specifies the VLAN identification. For the Cisco 2600, 3600, and 3700 series routers, the valid values are from 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094. For the Cisco 6500/6000 and 7600 series routers, valid values are 1 to 4094.
remote vlan *rspan-vlan-id*	Specifies the RSPAN VLAN as a destination VLAN.
destination	Specifies the SPAN-destination interface.
analysis-module *slot-number*	Specifies the network analysis module number; see the "Usage Guidelines" section for additional information.
data-port *port-number*	Specifies the data port number; see the "Usage Guidelines" section for additional information.

filter vlan *vlan-range*	Limits SPAN-source traffic to specific VLANs. **Note** The **filter** keyword is not supported on the Cisco 2600 series or the Cisco 3600 series routers.
servicemodule	Specifies service modules. See the "Usage Guidelines" for a list of the valid values.
mod-list	List of service module numbers.
type erspan-destination	Enters the ERSPAN destination-session configuration mode. See the **monitor session type** command for additional information.
type erspan-source	Enters the ERSPAN source-session configuration mode. See the **monitor session type** command for additional information.
range *session-range*	Specifies the range of sessions.
local	Specifies the local session.
remote	Specifies the remote session.
all	Specifies all sessions.

Command Default

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

A trunking interface monitors all VLANs and all received and transmitted traffic.

Cisco 6500/6000 Catalyst Switches and 7600 Series Routers

The defaults are as follows:

- **both**—Received and transmitted traffic are monitored.
- **servicemodule**—All service modules are allowed to use the SPAN service module session.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
12.1(1)E	Support for this command on the Catalyst 6000 family switches was extended to Cisco IOS Release 12.1(1)E.
12.1(3a)E3	The number of valid values for the port-channel number was changed; see the "Usage Guidelines" section for valid values.
12.1(5c)EX	These SPAN support restrictions were added: • If your switch has a Switch Fabric Module installed, SPAN is supported among supervisor engines and nonfabric-enabled modules. • If your switch does not have a Switch Fabric Module installed, SPAN is supported on all modules, including fabric-enabled modules. • SPAN on DFC-equipped modules is not supported.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to support the SSO mode and change the default mode.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720 only: • Added the **type erspan-source** and the **type erspan-source** keywords to support ERSPAN; see the **monitor session type** command for additional information. • Added the *mod-list* argument to the **monitor session servicemodule** command to allow you to enable or disable the SPAN service module session for a list of modules. • In the transmit or transmit and receive directions, you can specify up to 128 physical interfaces as the source.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs to 1–4094 for specified platforms.

Usage Guidelines

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

The **port-channel** *number* supports six EtherChannels and eight ports in each channel.

Only one SPAN destination for a SPAN session is supported. If you attempt to add another destination interface to a session that already has a destination interface configured, you will get an error. You must first remove a SPAN destination interface before changing the SPAN destination to a different interface.

Ciso 6500/6000 Catalyst Switches

The number of valid values for **port-channel** *number* depends on the software release. For Cisco IOS releases prior to software Release 12.1(3a)E3, valid values are from 1 to 256; for Cisco IOS Release 12.1(3a)E3, 12.1(3a)E4, and 12.1(4)E1, valid values are from 1 to 64. Cisco IOS Release 12.1(5c)EX and later support a maximum of 64 values ranging from 1 to 256.

Only one destination per SPAN session is supported. If you attempt to add another destination interface to a session that already has a destination interface configured, you get an error. You must first remove a SPAN destination interface before changing the SPAN destination to a different interface.

You can configure up to 64 SPAN destination interfaces, but you can have one egress SPAN source interface and up to 64 ingress source interfaces only.

A SPAN session can either monitor VLANs or monitor individual interfaces, but it cannot monitor both specific interfaces and specific VLANs. Configuring a SPAN session with a source interface and then trying to add a source VLAN to the same SPAN session causes an error. Configuring a SPAN session with a source VLAN and then trying to add a source interface to that session also causes an error. You must first clear any sources for a SPAN session before switching to another type of source.

If you enter the **filter** keyword on a monitored trunk interface, only traffic on the set of specified VLANs is monitored.

Port channel interfaces display in the list of **interface** options if you have them configured. VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **monitor session** *session* **source vlan** *vlan-id* command.

The following **servicemodule** *mod-list* values are valid for the Cisco 6500/6000 Catalyst switches:

- **bpdu**—Enables Bridge Protocol Data Units (BPDUs) of service modules.
- **module**—Specifies a list of service modules.
- **network-analysis-module**—Enables Network Analysis Module (NAM) service module.

Cisco 7600 Series Routers

Use these formatting guidelines when configuring monitor sessions:

- *interface* and *single-interface* formats are *type slot/port*; valid values for *type* are **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- An *interface-list* is a list of interfaces that are separated by commas. Insert a space before and after each comma as shown in this example:

  single-interface , *single-interface* , *single-interface*
- An *interface-range* is a range of interfaces that are separated by dashes. Insert a space before and after each dash. To enter multiple ranges, separate each range with a comma as shown in this example:

  type slot/first-port , *last-port*
- A *mixed-interface-list* is a mixed list of interfaces. Insert a space before and after each dash and comma as shown in this example:

  single-interface, - *interface-range* , ... in any order.
- A *single-vlan* is an ID number of a single VLAN; valid values are from 1 to 4094.
- A *vlan-list* is a list of VLAN IDs that are separated by commas. An example is shown as follows:

  single-vlan , *single-vlan* , *single-vlan* ...
- A *vlan-range* is a range of VLAN IDs that are separated by dashes. An example is shown as follows:

  first-vlan-ID - last-vlan-ID
- A *mixed-vlan-list* is a mixed list of VLAN IDs. Insert a space before and after each dash. To enter multiple ranges, separate each VLAN ID with a comma as shown in this example:

  single-vlan , *vlan-range* , ... in any order
- The servicemodule keyword has only one valid value:
  - **module**—Specifies a list of service modules.

The **analysis-module** *slot-number* and the **data-port** *port-number* keywords and arguments are supported only on NAM.

The number of valid values for **port-channel** *number* are a maximum of 64 values ranging from 1 to 256.

You cannot share the destination interfaces among SPAN sessions. For example, a single destination interface can belong to one SPAN session only and cannot be configured as a destination interface in another SPAN session.

Note Be careful when configuring SPAN-type source ports that are associated to SPAN-type destination ports because you do not configure SPAN on high-traffic interfaces. If you configure SPAN on high-traffic interfaces, you may saturate fabric channels, replication engines, and interfaces. To configure SPAN-type source ports that are associated to SPAN-type destination ports, enter the **monitor session** *session* **source** {**interface** *type* | **vlan** *vlan-id* [**rx** | **tx** | **both**] | **remote vlan** r*span-vlan-id*} command.

The Supervisor Engine 720 local SPAN, RSPAN, and ERSPAN session limits are listed in Table 2.

Table 2 Supervisor Engine 720 Local SPAN, RSPAN, and ERSPAN Session Limits

Total Sessions	Local SPAN, RSPAN Source, or ERSPAN Source Sessions	RSPAN Destination Sessions	ERSPAN Destination Sessions
66	2 (ingress or egress or both)	64	23

The Supervisor Engine 720 local SPAN, RSPAN, and ERSPAN source and destination limits are listed in Table 3.

Table 3 Supervisor Engine 720 Local SPAN, RSPAN, and ERSPAN Source and Destination Limits

	In Each Local SPAN Session	In Each RSPAN Source Session	In Each ERSPAN Source Session	In Each RSPAN Destination Session	In Each ERSPAN Destination Session
Egress or ingress and egress sources				—	—
With releases earlier than Release 12.2(18)SXE	1	1	1		
Release 12.2(18)SXE and later releases	128	128	128		
Ingress sources				—	—
With releases earlier than Release 12.2(18)SXD	64	64	64		
Release 12.2(18)SXD and later releases	128	128	128		
RSPAN and ERSPAN destination session sources	—	—	—	1 RSPAN VLAN	1 IP address
Destinations per session	64	1 RSPAN VLAN	1 IP address	64	64

Note

- Supervisor Engine 2 does not support RSPAN if you configure an egress SPAN source for a local SPAN session.
- Supervisor Engine 2 does not support egress SPAN sources for local SPAN if you configure RSPAN.

The Supervisor Engine 2 local SPAN and RSPAN session limits are listed in Table 4.

Table 4 Supervisor Engine 2 Local SPAN and RSPAN Session Limits

Total Sessions	Local SPAN Sessions	RSPAN Source Sessions	RSPAN Destination Sessions
66	2 (ingress or egress or both)	0	64
	1 ingress	1 (ingress or egress or both)	64
	1 or 2 egress	0	64

The Supervisor Engine 2 local SPAN and RSPAN source and destination limits are listed in Table 5.

Table 5 Supervisor Engine 2 Local SPAN and RSPAN Source and Destination Limits

	In Each Local SPAN Session	In Each RSPAN Source Session	In Each RSPAN Destination Session
Egress or egress and ingress sources	1 (0 with a remote SPAN source session configured)	1 (0 with a local SPAN egress source session configured)	—
Ingress sources			—
With releases earlier than Release 12.2(18)SXD	64	64	
Release 12.2(18)SXD and later releases	128	128	
RSPAN destination session source	—	—	1 RSPAN VLAN
Destinations per session	64	1 RSPAN VLAN	64

Note Supervisor Engine 2 does not support RSPAN if you configure an egress SPAN source for a local SPAN session.

Note Supervisor Engine 2 does not support egress SPAN sources for local SPAN if you configure RSPAN.

A particular SPAN session can either monitor the VLANs or monitor individual interfaces—you cannot have a SPAN session that monitors both specific interfaces and specific VLANs. If you first configure a SPAN session with a source interface, and then try to add a source VLAN to the same SPAN session, you get an error. You also get an error if you configure a SPAN session with a source VLAN and then try to add a source interface to that session. You must first clear any sources for a SPAN session before switching to another type of source.

If you enter the **filter** keyword on a monitored trunk interface, only traffic on the set of specified VLANs is monitored.

The port-channel interfaces display in the list of **interface** options if you have them configured. The VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **monitor session** *session* **source vlan** *vlan-id* command.

The **show monitor** command displays the SPAN service module session only if it is allocated in the system. It also displays a list of allowed modules and a list of active modules that can use the service module session.

Only the **no** form of the **monitor session servicemodule** command is displayed when you enter the **show running-config** command.

If no module is allowed to use the service module session, the service module session is automatically deallocated. If at least one module is allowed to use the service module session and at least one module is online, the service module session is automatically allocated.

If you allow or disallow a list of modules that are not service modules from using the service module session, there will be no effect on the allocation or deallocation of the service module session. Only the list of modules is saved in the configuration.

If you disable the SPAN service module session with the **no monitor session sericemodule** command, allowing or disallowing a list of modules from using the service module session has no effect on the allocation or deallocation of the service module session. Only the list of modules is saved in the configuration.

The **monitor session sericemodule** command is accepted even if there are no modules physically inserted in any slot.

Examples

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

The following example shows how to add a destination VLAN to an existing SPAN session:

```
Router(config)# monitor session 1 destination interface fastEthernet 2/0
```

Cisco 6500/600 Catalyst Switches

The following example shows how to add a destination VLAN to an existing SPAN session:

```
Router(config)# monitor session 1 destination vlan 100
```

The following example shows how to delete a destination VLAN from an existing SPAN session:

```
Router(config)# no monitor session 1 destination vlan 100
```

The following example shows how to limit SPAN traffic to specific VLANs:

```
Router(config)# monitor session 1 filter vlan 100 - 304
```

Cisco 7600 Series Routers

This example shows how to configure multiple sources for a session:

```
Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

This example shows how to configure an RSPAN destination in the final switch (RSPAN destination session):

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface fastethernet 1/2 , 2/3
```

This example shows how to clear the configuration for sessions 1 and 2:

```
Router(config)# no monitor session 1 - 2
Router(config)#
```

This example shows how to clear the configuration for all sessions:

```
Router(config)# no monitor session all
Router(config)#
```

This example shows how to clear the configuration for all remote sessions:

```
Router(config)# no monitor session remote
Router(config)#
```

This example shows how to allow a list of modules to use the SPAN service module session:

```
Router(config)# monitor session servicemodule module 1 - 2
Router(config)#
```

This example shows how to disallow a list of modules from using the SPAN service module session:

```
Router(config)# no monitor session servicemodule module 1 - 2
Router(config)#
```

Related Commands

Command	Description
remote-span	Configures a VLAN as an RSPAN VLAN.
show monitor	Displays SPAN session information.
show monitor session	Displays information about the ERSPAN, SPAN, and RSPAN sessions.

mvrp global

To enable Multiple VLAN Registration Protocol (MVRP) globally on a device and on a specified interface, use the **mvrp global** command in global configuration mode. To disable MRVP, use the **no** form of this command.

mvrp global

no mvrp global

Syntax Description

This command has no arguments or keywords.

Command Default

MVRP is administratively disabled.
MRVP is administratively enabled on each interface.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

MVRP is operational on an interface only if MVRP is administratively enabled both globally at the device level and at the interface level.

When MVRP is operational on an interface MVRP protocol data units (PDUs) are transmitted out the interface which must be a forwarding IEEE 802.1Q trunk. Other MVRP-related operations can then be enabled on the interface.

Examples

The following example configures global MVRP on the device and interfaces:

```
Router> enable
Router# configure terminal
Router(config)# mvrp global
%MVRP is now globally enabled. MVRP is operational on 802.1q trunk ports only.
Router(config)# interface fastethernet2/1
Router(config-if)# exit
Router(config)# mvrp global
Router(config)# interface fastethernet2/2
Router(config-if)# exit
Router(config)# mvrp global
Router(config)# end
```

Related Commands

Command	Description
clear mvrp statistics	Clears MVRP-related statistics recorded on one or all MVRP-enabled ports.
debug mvrp	Displays MVRP debugging information.
mvrp mac-learning auto	Enables MVRP to provision MAC address learning.
mvrp registration	Sets the registrars in a MAD instance associated with an interface.
mvrp timer	Sets period timers that are used in MRP on a specified interface.
mvrp vlan create	Enables an MVRP dynamic VLAN.
show mvrp interface	Displays details of the administrative and operational MVRP states of all or one particular IEEE 802.1Q trunk port in the device.
show mvrp summary	Displays the MVRP configuration at the device level.

mvrp mac-learning

To enable automatic learning of dynamic MAC table entries, use the **mvrp mac-learning** command in global configuration mode. To disable automatic learning of dynamic MAC table entries, use the **no** form of this command.

mvrp mac-learning auto

no mvrp mac-learning auto

Syntax Description

auto	Enables automatic MAC learning on VLANs that are configured with Multiple VLAN Registration Protocol (MVRP).

Command Default

Automatic MAC learning is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

With this command you can allow or disallow MVRP to provision MAC learning on devices where MVRP is configured. Automatic MAC learning is disabled by default.

Examples

The following example enable automatic learning of dynamic MAC table entries:

```
Router(config)# mvrp mac-learning auto
```

Related Commands

Command	Description
mvrp global	Enables MVRP globally on a device.

mvrp registration

To set the registrars in a Multiple Registration Protocol (MRP) Attribute Declaration (MAD) instance associated with an interface, use the **mvrp registration** command in global configuration mode. To disable the registrars, use the **no** form of this command.

mvrp registration {**normal** | **fixed** | **forbidden**}

no mvrp registration

Syntax Description

normal	Registrar responds normally to incoming Multiple VLAN Registration Protocol (MVRP) messages. Normal is the default state.
fixed	Registrar ignores all incoming MVRP messages and remains in the IN state.
forbidden	Registrar ignores all incoming MVRP messages and remains in the EMPTY (MT) state.

Command Default

Registrars are set to the normal state.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **mvrp registration** command is operational only if MVRP is configured on an interface.

The **no mvrp registration** command sets the registrar state to the default (normal).

This command can be used to set the registrar in a MAD instance associated with an interface to one of the three states. This command is effective only if MVRP is operational on the interface.

Given that up to 4094 VLANs can be configured on a trunk port, there may be up to 4094 Advanced Services Module (ASM) and Route Switch Module (RSM) pairs in a MAD instance associated with that interface.

Examples

The following example sets a fixed, forbidden, and normal registrar on a MAD instance:

```
Router(config)# mvrp global
%MVRP is now globally enabled. MVRP is operational on IEEE 802.1q trunk ports only.
Router(config)# interface fastethernet2/1
Router(config-if)# mvrp registration fixed
Router(config-if)# interface fastethernet2/2
Router(config-if)# mvrp registration forbidden
Router(config-if)# interface fastethernet2/3
Router(config-if)# no mvrp registration
```

Related Commands

Command	Description
clear mvrp statistics	Clears MVRP-related statistics recorded on one or all MVRP-enabled ports.
debug mvrp	Displays MVRP debugging information.
mvrp global	Enables MVRP globally on a device and on a particular interface.
mvrp mac-learning auto	Enables automatic learning of MAC table entries by MVRP.
mvrp timer	Sets period timers that are used in MRP on a given interface.
mvrp vlan create	Enables an MVRP dynamic VLAN.
show mvrp interface	Displays details of the administrative and operational MVRP states of all or one particular IEEE 802.1Q trunk port in the device.
show mvrp summary	Displays the MVRP configuration at the device level.

mvrp timer

To set period timers that are used in Multiple VLAN Registration Protocol (MVRP) on a given interface, use the **mvrp timer** command in interface configuration mode. To remove the timer value, use the **no** form of this command.

mvrp timer {**join** | **leave** | **leave-all** | **periodic**} [*centiseconds*]

no mvrp timer

Syntax Description

join	Specifies the time interval between two transmit opportunities that are applied to the Applicant State Machine (ASMs).
leave	Specifies the duration time before a registrar is moved to EMPTY (MT) state from leave-all (LV) state.
leave-all	Specifies the time it takes for a LeaveAll timer to expire.
periodic	Sets the timer value to periodic, a fixed value of 100 centiseconds.
centiseconds	Timer value measured in centiseconds. • Join timer value range is 20 to 10000000. • Leave timer value range is 60 to 10000000. • LeaveAll timer value range is 10000 and 10000000. • Periodic timer value is fixed at 100 centiseconds.

Command Default

Join timer value: 20 centiseconds
Leave timer value: 60 centiseconds
LeaveAll timer value: 10000 centiseconds

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **no mvrp timer** command resets the timer value to the default value.

Examples

The following example sets the timer levels on an interface:

```
Router(config)# mvrp global
%MVRP is now globally enabled. MVRP is operational on IEE 802.1q trunk ports.
Router(config)# interface GigabitEthernet 6/1
Router(config-if)# mvrp timer join 30
Router(config-if)# mvrp timer leave 70
Router(config-if)# mvrp timer leaveAll 15000
```

Related Commands

Command	Description
clear mvrp statistics	Clears MVRP-related statistics recorded on one or all MVRP enabled ports.
debug mvrp	Displays MVRP debugging information.
mvrp global	Enables MVRP globally on a device and on a particular interface.
mvrp mac-learning auto	Enables automatic learning of MAC table entries by MVRP.
mvrp registration	Sets the registrars in a MAD instance associated with an interface.
mvrp vlan create	Enables an MVRP dynamic VLAN.
show mvrp interface	Displays details of the administrative and operational MVRP states of all or one particular IEEE 802.1q trunk port in the device.
show mvrp summary	Displays the MVRP configuration at the device level.

mvrp vlan creation

To enable dynamic VLAN creation on a device using Multiple VLAN Registration Protocol (MVRP), use the **mvrp vlan creation** command in global configuration mode. To disable dynamic VLAN creation for MVRP, use the **no** form of this command.

mvrp vlan creation

no mvrp vlan creation

Syntax Description

This command has no arguments or keywords.

Command Default

MVRP is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

MVRP dynamic VLAN creation can be used only if Virtual Trunking Protocol (VTP) is in transparent mode.

Examples

The following example shows a command sequence enabling MVRP dynamic VLAN creation. Notice that the device recognizes that the VTP mode is incorrect and rejects the request for dynamic VLAN creation. Once the VTP mode is changed, MVRP dynamic VLAN creation is allowed.

```
Router(config)# mvrp vlan creation
%Command Rejected: VTP is in non-transparent (server) mode.
Router(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Router(config)# mvrp vlan creation
%VLAN now may be dynamically created via MVRP/
```

Related Commands

Command	Description
mvrp global	Enables MVRP globally on a device.
vtp mode	Sets the mode for VTP mode on the device.

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.

Defaults

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.

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 Catalyst 6500 series switch in a different region. The configuration name is a case-sensitive parameter.

Examples

This example shows how to name a region:

```
Router(config-mst)# name Cisco
Router(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.

pagp learn-method

To learn the input interface of the incoming packets, use the **pagp learn-method** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

pagp learn-method {**aggregation-port** | **physical-port**}

no pagp learn-method

Syntax Description

aggregation-port	Specifies how to learn the address on the port channel.
physical-port	Specifies how to learn the address on the physical port within the bundle.

Defaults

The default is **aggregation-port**.

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(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.

Examples

This example shows how to set the learning method to learn the address on the physical port within the bundle:

```
Router(config-if)# pagp learn-method physical-port
Router(config-if)#
```

This example shows how to set the learning method to learn the address on the port channel within the bundle:

```
Router(config-if)# pagp learn-method aggregation-port
Router(config-if)#
```

Related Commands

Command	Description
show pagp	Displays port-channel information.

pagp port-priority

To select a port in hot standby mode, use the **pagp port-priority** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

pagp port-priority *priority*

no pagp port-priority

Syntax Description

priority	Priority number; valid values are from 1 to 255.

Defaults

priority is **128**.

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(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.

Usage Guidelines

The higher the priority means the better the chances are that the port will be selected in the hot standby mode.

Examples

This example shows how to set the port priority:

```
Router(config-if)# pagp port-priority 45
Router(config-if)#
```

Related Commands

Command	Description
pagp learn-method	Learns the input interface of the incoming packets.
show pagp	Displays port-channel information.

port-channel load-defer

To configure the port load share deferral interval for all port channels, use the **port-channel load-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

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

Defaults

The port defer interval is 120 seconds.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

To reduce data loss following a stateful switchover (SSO), port load share deferral can be enabled by entering the **port-channel port load-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-channel load-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.

port-channel port load-defer

To enable the temporary deferral of port load sharing during the connection or reconnection of a port channel, use the **port-channel port load-defer** command in interface configuration mode. To disable the deferral of port load sharing on a port channel, use the **no** form of this command.

port-channel port load-defer

no port-channel port load-defer

Syntax Description

This command has no keywords or arguments.

Defaults

The port load share deferral feature is not enabled on a port channel.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

To reduce data loss following a stateful switchover (SSO), a port load share deferral can be enabled on a port channel of a switch that is connected by a multichassis EtherChannel (MEC) to a virtual switching system (VSS). The load share deferral interval 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.

When load share deferral is enabled on a port channel, the assignment of a member port's load share is delayed for a period that is configurable globally by the **port-channel load-defer** command. During the deferral period, the load share of a deferred member port is set to 0. In this state, the deferred port is capable of receiving data and control traffic, and of sending control traffic, but the port is prevented from sending data traffic over the MEC to the VSS. Upon expiration of the global deferral timer, the deferred member port exits the deferral state and the port assumes its normal configured load share.

Load share deferral is applied only if at least one other member port of the port channel is currently active with a nonzero load share. If a port enabled for load share deferral is the first member bringing up the EtherChannel, the deferral feature does not apply and the port will forward traffic immediately.

The load share deferral interval is determined by a single global timer configurable from 1 to 1800 seconds by the **port-channel load-defer** command. The default interval is 120 seconds. 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.

Examples

This example shows how to enable the load share deferral feature on port channel 50 of a switch that is an MEC peer to a VSS:

```
Router(config)# interface port-channel 50
Router(config-if)# port-channel port load-defer
This will enable the load share deferral feature on this port-channel.
The port-channel should connect to a Virtual Switch (VSS).
Do you wish to proceed? [yes/no]: yes
Router(config-if)#
```

This example shows how to verify the state of the port deferral feature 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 = 120 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 load-defer	Configures the global port load share deferral time interval for port channels.
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 **no shutdown** commands.

Caution If you enter the **shutdown** command and then the **no shutdown** 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.

private-vlan association

To create an association between private VLANs (PVLANs), use the **private-vlan association** command in VLAN configuration mode. To remove the association, use the **no** form of this command.

private-vlan association {*private-vlan-list* | **add** *private-vlan-list* | **remove** *private-vlan-list*}

no private-vlan association

Syntax Description

private-vlan-list	VLAN ID of the PVLANs.
add	Associates a PVLAN with another PVLAN.
remove	Clears the association between PVLANs.

Command Default

No PVLANs are associated.

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 **no shutdown** commands.

Caution If you enter the **shutdown** command and then the **no shutdown** command in the VLAN configuration mode on a PVLAN (primary or secondary), the PVLAN type and association information can be deleted. Be sure 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.

VLAN 1 or VLANs ranging from 1002 to 1005 cannot be configured as PVLANs. Extended VLANs (VLAN IDs 1006 to 4094) can belong to PVLANs.

A PVLAN is a set of private ports that are characterized by using a common set of VLAN number pairs. Each pair is made up of at least two special unidirectional VLANs, and it is used by isolated ports, or by a community of ports to communicate with routers, or both.

VLAN Trunking Protocol (VTP) must be set to transparent mode to support PVLANs. After the PVLAN configuration, you must not change the VTP mode to client or server mode. VTP does not propagate PVLAN configuration. Each protected or private port is associated with a PVLAN, which is not supported through VTP. Therefore, you must configure PVLANs on each device where you require PVLAN ports.

A primary VLAN can contain one isolated VLAN and multiple community VLANs associated with it. An isolated or community VLAN can have only one primary VLAN associated with it.

Note The **private-vlan association** command does 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 create a PVLAN relationship between the primary VLAN 14, the isolated VLAN 19, and the community VLANs 20 and 21:

```
Router(config)# vlan 19
Router(config-vlan)# private-vlan isolated
Router(config-vlan)# exit
Router(config)# vlan 20
Router(config-vlan)# private-vlan community
Router(config-vlan)# exit
Router(config)# vlan 21
Router(config-vlan)# private-vlan community
Router(config-vlan)# exit
Router(config)# vlan 14
Router(config-vlan)# private-vlan primary
Router(config-vlan)# private-vlan association 19-21
```

The following example shows how to remove an isolated VLAN 19 and community VLAN 20 from the PVLAN association:

```
Router(config)# vlan 14
Router(config-vlan)# private-vlan association remove 19,20
```

Related Commands

Command	Description
private-vlan	Configures PVLANS.
show vlan	Displays VLAN information.
show vlan private-vlan	Displays PVLAN information.
vlan (VLAN)	Configures a specific VLAN.

private-vlan mapping

To create a mapping between the primary and the secondary VLANs so that both VLANs share the same primary VLAN switched virtual interface (SVI), use the **private-vlan mapping** command in interface configuration mode. To remove all private VLAN (PVLAN) mappings from the SVI, use the **no** form of this command.

private-vlan mapping [*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*]

no private-vlan mapping

Syntax Description

secondary-vlan-list	(Optional) VLAN IDs of the secondary VLANs to map to the primary VLAN.
add	(Optional) Maps the secondary VLAN to the primary VLAN.
remove	(Optional) Removes the mapping between the secondary VLAN and the primary VLAN.

Defaults

No PVLAN SVI mapping is configured.

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

Usage Guidelines

The **private-vlan mapping** command affects traffic that is switched in the software on the Multilayer Switching Feature Card (MSFC) or MSFC2. The **private-vlan mapping** command does not configure Layer 3 switching on the Policy Feature Card (PFC) or PFC2.

The *secondary-vlan-list* argument cannot contain spaces; it can contain multiple comma-separated items. Each item can be a single PVLAN ID or a hyphenated range of PVLAN IDs.

This command is valid in the interface configuration mode of the primary VLAN.

The SVI of the primary VLAN is created at Layer 3.

Traffic that is received on the secondary VLAN is routed by the SVI of the primary VLAN.

The SVIs of existing secondary VLANs do not function and are considered as down after you enter this command.

A secondary SVI can only be mapped to one primary SVI. If you configure the primary VLAN as a secondary VLAN, all the SVIs that are specified in this command are brought down.

If you configure a mapping between two VLANs that do not have a valid Layer 2 association, the mapping configuration does not take effect.

Examples

This example shows how to permit routing of secondary VLAN-ingress traffic from PVLANs 303 through 307, 309, and 440 and verify the configuration:

```
Router# configure terminal
Router(config)# interface vlan 202
Router(config-if)# private-vlan mapping add 303-307,309,440
Router(config-if)# end
Router# show interfaces private-vlan mapping

Interface Secondary VLAN Type
--------- -------------- -----------------
vlan202   303            community
vlan202   304            community
vlan202   305            community
vlan202   306            community
vlan202   307            community
vlan202   309            community
vlan202   440            isolated
Router#
```

This example shows the displayed error message if the VLAN that you are adding is already mapped to the SVI of VLAN 19. You must delete the mapping from the SVI of VLAN 19 first.

```
Router(config)# interface vlan 19
Router(config-if)# private-vlan mapping 19 add 21

    Command rejected: The interface for VLAN 21 is already mapped as s secondary.
Router(config-if)#
```

This example shows how to remove all PVLAN mappings from the SVI of VLAN 19:

```
Router(config)# interface vlan 19
Router(config-if)# no private-vlan mapping
Router(config-if)#
```

Related Commands

Command	Description
show interfaces private-vlan mapping	Displays the information about the PVLAN mapping for VLAN SVIs.
show vlan	Displays VLAN information.
show vlan private-vlan	Displays PVLAN information.

private-vlan synchronize

To map the secondary VLANs to the same instance as the primary VLAN, use the **private-vlan synchronize** command in MST configuration submode.

private-vlan synchronize

Syntax Description

This command has no arguments or keywords.

Defaults

The secondary VLANs are not mapped to the same instance as the primary VLAN.

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.

Usage Guidelines

If you do not map VLANs to the same instance as the associated primary VLAN when you exit the Multiple Spanning Tree (802.1s) (MST) configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The **private-vlan synchronize** command automatically maps all secondary VLANs to the same instance as the associated primary VLANs.

Examples

This example assumes that a primary VLAN 2 and a secondary VLAN 3 are associated to VLAN 2, and that all VLANs are mapped to the Common and Internal Spanning Tree (CIST) instance 1. This example also shows the output if you try to change the mapping for the primary VLAN 2 only:

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 2
Router(config-mst)# exit

These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

This example shows how to initialize private VLAN (PVLAN) synchronization:

```
Router(config-mst)# private-vlan synchronize
Router(config-mst)#
```

Related Commands

Command	Description
show	Verifies the MST configuration.
show spanning-tree mst	Displays information about the MST protocol.

rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit hardware flood layer (HFL) messages, use the **rep admin vlan** command in global configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

rep admin vlan *vlan-id*

no rep admin vlan

Syntax Description

vlan-id	The VLAN ID range is from 1 to 4094. The default is VLAN 1; the range to configure is 2 to 4094.

Defaults

The administrative VLAN is VLAN 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(40)SE	This command was introduced.
12.2(33)SRC	This command was implemented on the Cisco 7600 series router.
Cisco IOS XE Release 2.2	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Router.

Usage Guidelines

If the VLAN does not already exist, this command does not create the VLAN.

To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the HFL to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. Configuring an administrative VLAN for the whole domain can control flooding of these messages.

If no REP administrative VLAN is configured, the default is VLAN 1.

There can be only one administrative VLAN on a switch and on a segment.

The administrative VLAN cannot be the RSPAN VLAN.

Examples

This example shows how to configure VLAN 100 as the REP administrative VLAN:

```
Router(config)# rep admin vlan 100
```

You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

Related Commands

Command	Description
show interfaces rep detail	Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep block port

To configure Resilient Ethernet Protocol (REP) VLAN load balancing on the REP primary edge port, use the **rep block port** command in interface configuration mode. To return to the default configuration, use the **no** form of this command.

rep block port {id *port-id* **|** *neighbor-offset* **| preferred} vlan** {*vlan-list* **| all**}

no rep block port {**id** *port-id* **|** *neighbor-offset* **| preferred**}

Syntax Description

id *port-id*	Identify the VLAN blocking alternate port by entering the unique port ID that is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can display the port ID for an interface by entering the **show interface** *interface-id* **rep detail** command.
neighbor-offset	Identify the VLAN blocking alternate port by entering the offset number of a neighbor. The range is –256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number –1) and its downstream neighbors.
preferred	Identify the VLAN blocking alternate port as the segment port on which you entered the **rep segment** *segment-id* **preferred** interface configuration command. **Note** Entering the **preferred** keyword does not ensure that the preferred port is the alternate port; it gives it preference over other similar ports.
vlan	Identify the VLANs to be blocked.
vlan-list	The VLAN ID or range of VLAN IDs to be displayed. Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) of VLANs to be blocked.
all	Enter to block all VLANs.

Defaults

The default behavior after you enter the **rep preempt segment** privileged EXEC command (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(40)SE	This command was introduced.
12.2(33)SRC	This command was implemented on the Cisco 7600 series router.
Cisco IOS XE Release 2.2	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Router.

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number –1) and its downstream neighbors. You would never enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay** *seconds* interface configuration command and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. The port ID format is similar to the one used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). To determine the port ID of a port, enter the **show interfaces** *interface-id* **rep detail** privileged EXEC command.

Examples

This example shows how to configure REP VLAN load balancing on the Router B primary edge port (Gigabit Ethernet port 1/0/1) and to configure Gigabit Ethernet port 1/0/2 of Router A as the alternate port to block VLANs 1 to 100. The alternate port is identified by its port ID, shown in bold in the output of the **show interfaces rep detail** command for the Router A port.

```
RouterA# show interfaces gigabitethernet0/2 rep detail

GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB17800EEE
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 1
Preempt Delay Timer: 35 sec
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to:
PDU/TLV statistics:
LSL PDU rx: 107122, tx: 192493

RouterB# configure terminal
Router(config)# interface gigabitethernet1/0/1
Router(config-if)# rep block port id 0080001647FB1780 vlan 1-100
Router(config-if)# exit
```

This example shows how to configure VLAN load balancing by using a neighbor offset number and how to verify the configuration by entering the **show interfaces rep detail** privileged EXEC command:

```
Router# configure terminal
Router#(config)# interface gigabitethernet1/0/2
Router#(config-if)# rep block port 6 vlan 1-110
Router#(config-if)# end

Router# show interface gigabitethernet1/0/2 rep detail

GigabitEthernet0/2 REP enabled
```

```
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB178009C3
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 3
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
Load-balancing block vlan: 1-110
STCN Propagate to: none
LSL PDU rx: 1466780, tx: 3056637
HFL PDU rx: 2, tx: 0
BPA TLV rx: 1, tx: 2119695
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 757406, tx: 757400
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 178326, tx: 178323
```

Related Commands

Command	Description
rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
rep preempt segment	Manually starts REP VLAN load balancing on a segment.
show interfaces rep detail	Displays REP detailed configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep lsl-age-timer

To configure the Resilient Ethernet Protocol (REP) link status layer (LSL) age-out timer value, use the **rep lsl-age-timer** command in interface configuration mode. To restore the default age-out timer value, use the **no** form of this command.

rep lsl-age-timer *milliseconds*

no rep lsl-age-timer *milliseconds*

Syntax Description

milliseconds	Defines the REP LSL age-out timer value in milliseconds (ms). Range is from 120 ms to 10000 ms in multiples of 40 ms. The default is 5 ms.

Command Default

The default LSL age-out timer value is 5 ms.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)S	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

REP is a Cisco proprietary protocol that provides functionality to:

- Control network loops
- Handle link failures
- Improve convergence time

The **rep lsl-age-timer** command is used to configure the REP LSL age-out timer value.

Examples

The following example shows how to configure the REP LSL age-out timer value.

```
Router# enable
Router# configure terminal
Router(config)# interface gigabitethernet 5/3
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep lsl-age-timer 2000
Router(config-if)# exit
```

Related Commands

Command	Description
rep lsl-retries	Configures the number of retries before the REP link is disabled.

rep lsl-retries

To configure the Resilient Ethernet Protocol (REP) link status layer (LSL) number of retries, use the **rep lsl-retries** command in interface configuration mode. To restore the default number of retries, use the **no** form of this command.

rep lsl-retries *number-of-retries*

no rep lsl-retries *number-of-retries*

Syntax Description

number-of-retries	The number of LSL retries. The acceptable range is between 3 and 10 retries. The default number of retries is 5.

Command Default

The default number of retries is 5.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)S	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

REP is a Cisco proprietary protocol that provides functionality to:

- Control network loops
- Handle link failures
- Improve convergence time

The **rep lsl-retries** command is used to configure the number of retries before the REP link is disabled.

Examples

This example shows how to configure REP link status layer number of retries.

```
Router# enable
Router# configure terminal
Router(config)# interface gigabitethernet 2/5
Router(config-if)# rep segment 2 edge primary
Router(config-if)# rep lsl-retries 4
Router(config-if)# exit
```

Related Commands

Command	Description
rep lsl-age-timer	Configures the REP link status layer age-out timer value.

rep preempt delay

To configure a waiting period after a segment port failure and recovery before Resilient Ethernet Protocol (REP) VLAN load balancing is triggered, use the **rep preempt delay** command in interface configuration mode. To remove the configured delay, use the **no** form of this command.

rep preempt delay *seconds*

no rep preempt delay

Syntax Description

seconds	The number of seconds to delay REP preemption. The range is 15 to 300.

Defaults

No preemption delay is set. If you do not enter the **rep preempt delay** command, the default is manual preemption with no delay.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(40)SE	This command was introduced.
12.2(33)SRC	This command was implemented on the Cisco 7600 series router.
Cisco IOS XE Release2.2	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Router.

Usage Guidelines

You must enter this command on the REP primary edge port.

You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.

If VLAN load-balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge alerts the alternate port to perform VLAN load-balancing (configured by using the **rep block port** interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.

Examples

This example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port:

```
Router(config)# interface gigabitethernet1/0/1
Router(config-if)# rep preempt delay 100
Router(config-if)# exit
```

You can verify your settings by entering the **show interfaces rep** privileged EXEC command.

Related Commands

Command	Description
rep block port	Configures VLAN load balancing.
show interfaces rep	Displays REP configuration and status for all interfaces or the specified interface.

rep preempt segment

To manually start Resilient Ethernet Protocol (REP) VLAN load balancing on a segment, use the **rep preempt segment** command in privileged EXEC mode.

rep preempt segment *segment-id*

Syntax Description

segment-id	ID of the REP segment. The range is from 1 to 1024.

Defaults

Manual preemption is the default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(40)SE	This command was introduced.
12.2(33)SRC	This command was implemented on the Cisco 7600 series router.
Cisco IOS XE Release 2.2	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Router.

Usage Guidelines

After you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption can cause network disruption.

Enter this command on the router on the segment that has the primary edge port.

If you do not configure VLAN load balancing, entering this command results in the default behavior—the primary edge port blocks all VLANs.

You configure VLAN load balancing by entering the **rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**} interface configuration command on the REP primary edge port before you manually start preemption.

There is not a **no** version of this command.

Examples

This example shows how to manually trigger REP preemption on segment 100 with the confirmation message:

```
Router# rep preempt segment 100
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

Related Commands

Command	Description
rep block port	Configures VLAN load balancing.
show interfaces rep	Displays REP configuration and status for all interfaces or the specified interface.

rep segment

To enable Resilient Ethernet Protocol (REP) on the interface and to assign a segment ID to the interface, use the **rep segment** command in interface configuration mode. To disable REP on the interface, use the **no** form of this command.

rep segment *segment-id* [**edge [no-neighbor]** [**primary**]] [**preferred**]

no rep segment

Syntax Description

segment-id	The segment for which REP will be enabled. Assign a segment ID to the interface. The range is from 1 to 1024.
edge	(Optional) Identify the interface as one of the two REP edge ports. Entering the **edge** keyword without the **primary** keyword configures the port as the secondary edge port.
primary	(Optional) On an edge port, specify that the port is the primary edge port. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port (for example, ports on different switches) the REP selects one of them to serve as the segment primary edge port.
no-neighbor	(Optional) On an edge port, specify the segment edge as one with no external REP neighbor.
preferred	(Optional) Specify that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

Defaults

REP is disabled on the interface.
When REP is enabled on an interface, the default is for the port to be a regular segment port.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(40)SE	This command was introduced.
12.2(33)SRC	This command was implemented on the Cisco 7600 series router.
Cisco IOS XE Release 2.2	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Router.
15.1(01)S	This command was changed to add the **no-neighbor** keyword.

Usage Guidelines

REP ports must be Layer 2 trunk ports. A non-Ethernet Services (ES) REP port can be either an IEEE 802.1Q trunk port or an ISL trunk port.

REP ports should not be configured as one of these port types:

- Access port
- Private VLAN port
- Switched Port Analyzer (SPAN) destination port
- Tunnel port

You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port. If you configure two ports in a segment as the primary edge port (for example, ports on different switches) the configuration is allowed, but the REP selects one of them to serve as the segment primary edge port.

REP Edge No Neighbor

You can configure the non-rep switch facing ports as edge no- neighbor ports. These ports inherit the properties of edge ports, and overcome the limitation of not being able to converge quickly during a failure.

REP on EtherChannels

REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

REP Enabled on Two Ports

If you enable REP on two ports on a switch, the ports must both be either regular segment ports or edge ports. REP ports follow these rules:

- If only one port on a switch is configured in a segment, the port should be an edge port.
- If two ports on a switch belong to the same segment, both ports must be edge ports, or both ports must be regular segment ports.
- If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

If you configure two ports in a segment as the primary edge port (for example, ports on different switches) the REP selects one of them to serve as the segment primary edge port. Enter the **show rep topology** privileged EXEC command on a port in the segment to verify which port is the segment primary edge port.

REP Interfaces

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.

REP in Networks with Redundancy

You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

Examples

REP Enabled on a Nonedge Segment Port

This example shows how to enable REP on a regular (nonedge) segment port:

```
Router(config)# interface gigabitethernet0/1
Router(config-if)# rep segment 100
```

REP Enabled as Primary Edge Port

This example shows how to enable REP on a port and identify the port as the REP primary edge port:

```
Router(config)# interface gigabitethernet0/2
Router(config-if)# rep segment 100 edge primary
```

REP as Secondary Edge Port

This example shows how to enable REP on a port and identify the port as the REP secondary edge port:

```
Router(config)# interface gigabitethernet0/2
Router(config-if)# rep segment 100 edge
```

REP as Edge No-Neighbor Port

This example shows how to enable REP as an edge no-neighbor port:

```
Router(config)# interface gigabitethernet0/2
Router(config-if)# rep segment 1 edge no-neighbor primary
```

Verify Settings with the show interfaces rep Command

You can verify your settings by entering the **show interfaces rep** privileged EXEC command. To verify which port in the segment is the primary edge port, enter the **show rep topology** privileged EXEC command.

Related Commands

Command	Description
show interfaces rep	Displays REP configuration and status for all interfaces or the specified interface.
show rep topology	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

rep stcn

To configure a Resilient Ethernet Protocol (REP) edge port to send REP segment topology change notifications (STCNs) to another interface, to other segments, or to Spanning Tree Protocol (STP) networks, use the **rep stcn** command in interface configuration mode. To disable the sending of STCNs to the interface, segment, or STP network, use the **no** form of this command.

rep stcn {**interface** *interface-id* | **segment** *id-list* | **stp**}

no rep stcn {**interface** | **segment** | **stp**}

Syntax Description

interface *interface-id*	Identify a physical interface or port channel to receive STCNs.
segment *id-list*	Identify one REP segment or a list of segments to receive STCNs. The range is 1 to 1024. You can also configure a sequence of segments (for example 3-5, 77, 100).
stp	Send STCNs to an STP network.

Defaults

Transmission of STCNs to other interfaces, segments, or STP networks is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(40)SE	This command was introduced.
12.2(33)SRC	This command was implemented on the Cisco 7600 series router.
Cisco IOS XE Release 2.2	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Router.

Usage Guidelines

Enter this command on a segment edge port.

You use this command to notify other portions of the Layer 2 network of topology changes that occur in the local REP segment. This removes obsolete entries in the Layer 2 forwarding table in other parts of the network, which allows faster network convergence.

Examples

This example shows how to configure a REP edge port to send STCNs to segments 25 to 50:

```
Router(config)# interface gigabitethernet1/0/2
Router(config-if)# rep stcn segment 25-50
Router(config-if)# exit
```

You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

Related Commands

Command	Description
show interfaces rep	Displays REP configuration and status for all interfaces or the specified interface.

revision

To set the revision number for the Multiple Spanning Tree (802.1s) (MST) configuration, use the **revision** command in MST configuration submode. To return to the default settings, use the **no** form of this command.

revision *version*

no revision

Syntax Description

version	Revision number for the configuration; valid values are from 0 to 65535.

Defaults

version is **0**.

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.

Usage Guidelines

Two Cisco 7600 series routers that have the same configuration but different revision numbers are considered to be part of two different regions.

Caution Be careful when using the **revision** command to set the revision number of the MST configuration because a mistake can put the switch in a different region.

Examples

This example shows how to set the revision number of the MST configuration:

```
Router(config-mst)# revision 5
Router(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST configuration submode)	Sets the name of an MST region.
show	Verifies the MST configuration.
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree mst configuration	Enters MST-configuration submode.

set port flowcontrol

To set the receive flow-control value for a particular Gigabit Ethernet switching module port, use the **set port flowcontrol** command in privileged EXEC mode. To reset the receive flow-control value to the default, use the **no** form of this command.

set port flowcontrol {**receive** | **send**} [*module-number* | *port-number*] {**off** | **on** | **desired**}

no set port flowcontrol {**receive** | **send**} [*module-number* | *port-number*] {**off** | **on** | **desired**}

Syntax Description

receive	Indicates whether the port can receive administrative status from a remote device.
send	Indicates whether the local port can send administrative status to a remote device.
module-number	(Optional) Number of the module.
port-number	(Optional) Number of the port on the module.
off	When used with **receive**, it turns off an attached device's ability to send flow-control packets to a local port. When used with **send**, it turns off the local port's ability to send administrative status to a remote device.
on	When used with **receive**, it requires that a local port receive administrative status from a remote device. When used with **send**, the local port sends administrative status to a remote device.
desired	When used with **receive**, it allows a local port to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to, but may send flow-control packets. When used with **send**, the local port sends administrative status to a remote device if the remote device supports it.

Command Default

receive—off
send—desired

Default on multiplexed ports is **on**. The exception to these defaults applies to the 18-port Gigabit Ethernet switching module. For this module, the defaults are shown below:

- Ports 1–2—**send** is **off** and **receive** is **desired**
- Ports 3–18—**send** is **on** and **receive** is **desired**

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced and implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

This command is supported only on Gigabit Ethernet switching modules.

Examples

The following examples show how to use the **set port flowcontrol** command set.

The following example show how to set the port 5/1 flow-control receive administration status to **on** (port requires far end to send flow-control packets):

```
Router# set port flowcontrol receive 5/1 on
```

The following example show how to set the port 5/1 flow-control receive administration status to **desired** (port allows far end to send flow-control packets if far end supports it):

```
Router# set port flowcontrol receive 5/1 desired
```

The following example show how to set the port 5/1 flow-control receive administration status to **off** (port does not allow far end to send flow-control packets):

```
Router# set port flowcontrol receive 5/1 off
```

The following example show how to set port 5/1 flow-control send administration status t o **on** (port sends flow-control packets to far end):

```
Router# set port flowcontrol send 5/1 on
```

The following example show how to set port 5/1 flow-control send administration status to **desired** (port sends flow-control packets to far end if far end supports it):

```
Router# set port flowcontrol send 5/1 desired
```

The following example show how to set port 5/1 flow-control send administration status to **off** (port does not send flow-control packets to far end):

```
Router# set port flowcontrol send 5/1 off
```

Related Commands

Command	Description
show port flowcontrol	Displays per-port status information and statistics related to flow control.

set vlan

To group ports into a virtual LAN (VLAN), use the **set vlan** *vlan-number module/port* command in privileged EXEC mode.

set vlan *vlan-number module/port*

To set advanced VLAN options for VLANs, use the advanced keywords.

set vlan *vlan-number* [**name** *name*] [**type** {**ethernet** | **fddi** | **fddinet** | **trcrf** | **trbrf**}] [**state** {**active** | **suspend**}] [**sa-id** *sa-id*] [**mtu** *mtu*] [**ring** *hex-ring-number*] [**decring** *decimal-ring-number*] [**bridge** *bridge-number*] [**parent** *vlan-number*] [**mode** {**srt** | **srb**}] [**stp** {**ieee** | **ibm** | **auto**}] [**translation** *vlan-number*] [**backupcrf** {**off** | **on**}] [**aremaxhop** *hop-count*] [**stemaxhop** *hop-count*]

Syntax Description

vlan-number	Number identifying the VLAN.
module	Number of the module.
port	Number of the port on the module belonging to the VLAN; this argument does not apply to TRBRFs.
name *name*	(Optional) Defines a text string used as the name of the VLAN (1 to 32 characters).
type {**ethernet** | **fddi** | **fddinet** | **trcrf** | **trbrf**}	(Optional) Identifies the VLAN type. The default type is Ethernet.
state {**active** | **suspend**}	(Optional) Specifies whether the state of the VLAN is active or suspended. VLANs in suspended state do not pass packets. The default state is active.
sa-id *sa-id*	(Optional) Specifies the security association identifier. Possible values are 1 to 4294967294. The default is 100001 for VLAN1, 100002 for VLAN 2, 100003 for VLAN 3, and so on. T
mtu *mtu*	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use. Possible values are 576 to 18190.
ring *hex-ring-number*	(Optional) Specifies the logical ring number for Token Ring VLANs. Possible values are hexadecimal numbers 0x1 to 0xFFF. This argument is valid and required only when you define a TRCRF.
decring *decimal-ring-number*	(Optional) Specifies the logical ring number for Token Ring VLANs. Possible values are decimal numbers 1 to 4095. This argument is valid and required only when you define a TRCRF.
bridge *bridge-number*	(Optional) Specifies the identification number of the bridge. Possible values are hexadecimal numbers 0x1 to 0xF.
parent *vlan-number*	(Optional) Sets a parent VLAN. The range for *vlan-number* is 2 to 1005. This argument identifies the TRBRF to which a TRCRF belongs and is required when you define a TRCRF.
mode {**srt** | **srb**}	(Optional) Specifies the TRCRF bridging mode.
stp {**ieee** | **ibm** | **auto**}	(Optional) Specifies the Spanning Tree Protocol version for a TRBRF to use: source-routing transparent (ieee), source-route bridging (ibm), or automatic source selection (auto).

translation *vlan-number*	(Optional) Specifies a VLAN used to translate FDDIto Ethernet. Valid values are from 1 to 1005. This argument is not valid for defining or configuring Token Ring VLANs.
backupcrf {**off** | **on**}	(Optional) Specifies whether the TRCRF is a backup path for traffic.
aremaxhop *hop-count*	(Optional) Specifies the maximum number of hops for All-Routes Explorer frames. Possible values are 1 to 14. The default is 7. This argument is valid only when you define or configure TRCRFs.
stemaxhop *hop-count*	(Optional) Specifies the maximum number of hops for Spanning-Tree Explorer frames. Possible values are 1 to 14. The default is 7. This argument is valid only when you define or configure TRCRFs.

Command Default

The default configuration has all switched Ethernet ports and Ethernet repeater ports in VLAN 1. Additional defaults are:

- SAID: 100001 for VLAN 1, 100002 for VLAN 2, 100003 for VLAN 3, and so on
- Type: Ethernet
- MTU: 1500 bytes
- State: Active

Defaults for TRBRFs and TRCRFs are:

- TRBRF : 1005
- TRCRF: 1003
- MTU for TRBRFs and TRCRFs : 4472.
- State: Active.
- **aremaxhop**: 7
- **stemaxhop**: 7.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
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

You cannot use the **set vlan** command until the networking device is in Virtual Trunking Protocol (VTP) transparent mode (**set vtp mode**) or until a VTP domain name has been set (**set vtp**).

Valid MTU values for a Token Ring VLAN are 1500 or 4472. You can enter any value but it defaults to the next lowest valid value.

You cannot set multiple VLANs for Inter-Switch Link (ISL) ports using this command. The VLAN name can be from 1 to 32 characters in length. If you add a new VLAN, the VLAN number must be within the range of 2 to 1001. When you modify a VLAN, the valid range for the VLAN number is 2 to 1005.

On a new Token Ring VLAN, if you do not specify the parent parameter for a TRCRF, the default TRBRF (1005) is used.

Examples

The following example shows how to set VLAN 850 to include ports 4 through 7 on module 3. Because ports 4 through 7 were originally assigned to TRCRF 1003, the message reflects the modification of VLAN 1003.

```
Router# set vlan 850 3/4-7
VLAN 850 modified.
VLAN 1003 modified.
VLAN  Mod/Ports
---- ----------------------
850   3/4-7
```

Related Commands

Command	Description
clear vlan	Deletes an existing VLAN from a management domain.
show vlans	Displays VLAN subinterfaces.

set vlan mapping

To map 802.1Q virtual LANs (VLANs) to Inter-Switch Link (ISL) VLANs, use the **set vlan mapping** command in privileged EXEC mode.

set vlan mapping dot1q *1q-vlan-number* **isl** *isl-vlan-number*

Syntax Description

dot1q	Specifies the 802.1Q VLAN.
1q-vlan-number	Number identifying the 802.1Q VLAN; valid values are 1001 to 4095.
isl	Specifies the ISL VLAN.
isl-vlan-number	Number identifying the ISL VLAN; valid values are 1 to 1000.

Command Default

No 802.1Q-to-ISL mappings are defined.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
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

IEEE 802.1Q VLAN trunks support VLANs 1 through 4095. ISL VLAN trunks support VLANs 1 through 1000. The switch automatically maps 802.1Q VLANs 1000 and lower to ISL VLANs with the same number.

The native VLAN of the 802.1Q trunk cannot be used in the mapping.

Use this feature to map 802.1Q VLANs above 1000 to ISL VLANs. If you map an 802.1Q VLAN over 1000 to an ISL VLAN, the corresponding 802.1Q VLAN will be blocked. For example, if you map 802.1Q VLAN 2000 to ISL VLAN 200, then 802.1Q VLAN 200 will be blocked.

You can map up to seven VLANs. Only one 802.1Q VLAN can be mapped to an ISL VLAN. For example, if 802.1Q VLAN 800 has been automatically mapped to ISL VLAN 800, do not manually map any other 802.1Q VLANs to ISL VLAN 800.

You cannot overwrite existing 802.1Q VLAN mapping. If the 802.1Q VLAN number is in the mapping table, the command is aborted. You must first clear that mapping.

If *vlan-number* does not exist, then either of the following occurs:

- If the switch is in server or transparent mode, the VLAN is created with all default values.
- If the switch is in client mode, then the command proceeds without creating the VLAN. A warning is given indicating that the VLAN does not exist.

If the table is full, the command is aborted with an error message indicating the table is full.

Examples

The following example shows how to map VLAN 1022 to ISL VLAN 850:

```
Router# set vlan mapping dot1q 1022 isl 850
Vlan 850 configuration successful
Vlan mapping successful
```

The following example shows the display if you enter a VLAN that does not exist:

```
Router# set vlan mapping dot1q 1017 isl 999
Vlan mapping successful
Warning: vlan 999 non-existent
Vlan 999 configuration successful
```

The following example shows the display if you enter an existing mapping:

```
Router# set vlan mapping dot1q 1033 isl 722
722 exists in the mapping table. Please clear the mapping first.
```

The following example shows the display if the mapping table is full:

```
Router# set vlan mapping dot1q 1099 isl 917
Vlan Mapping Table Full.
```

Related Commands

Command	Description
clear vlan mapping	Deletes existing 802.1Q VLAN to ISL VLAN-mapped pairs.
show vlans	Displays VLAN subinterfaces.

show

To verify the Multiple Spanning Tree (MST) configuration, use the **show** command in MST configuration mode.

show [**current** | **pending**]

Syntax Description

current	(Optional) Displays the current configuration that is used to run MST.
pending	(Optional) Displays the edited configuration that will replace the current configuration.

Command Default

This command has no default settings.

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.

Usage Guidelines

The display output from the **show pending** command is the edited configuration that will replace the current configuration if you enter the **exit** command to exit MST configuration mode.

Entering the **show** command with no arguments displays the pending configurations.

Examples

This example shows how to display the edited configuration:

```
Router(config-mst)# show pending

Pending MST configuration
Name      [zorglub]
Version   31415
Instance  Vlans Mapped
--------  ---------------------------------------------------------------------
0         4001-4096
2         1010, 1020, 1030, 1040, 1050, 1060, 1070, 1080, 1090, 1100, 1110
          1120
3         1-1009, 1011-1019, 1021-1029, 1031-1039, 1041-1049, 1051-1059
          1061-1069, 1071-1079, 1081-1089, 1091-1099, 1101-1109, 1111-1119
          1121-4000
-------------------------------------------------------------------------------
Router(config-mst)#
```

This example shows how to display the current configuration:

```
Router(config-mst)# show current

Current MST configuration
Name []
Revision 0
Instance Vlans mapped
-------- ---------------------------------------------------------------------
0 1-4094
---------------------------------------------------------------------------------
```

Related Commands

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

show controllers fastethernet

To display information about initialization block, transmit ring, receive ring, Fast Ethernet interface information, applicable MAC destination address and VLAN filtering tables, and errors for the Fast Ethernet controller chip, use the **show controllers fastethernet** command in user EXEC or privileged EXEC mode.

Standard Syntax

show controllers fastethernet *number*

Cisco 7200 Series

show controllers fastethernet *slot*/*port*

Cisco 7500 Series

show controllers fastethernet *slot*/*port-adapter*/*port*

Shared Port Adapter

show controllers fastethernet *slot*/*subslot*/*port* [**detail**]

Syntax Description

number	Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 router, specifies the network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system.
slot	Slot number. Refer to the appropriate hardware manual for slot information.
/*port*	Port number. Refer to the appropriate hardware manual for port information.
/*port-adapter*	Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.
/*subslot*	(Optional) Secondary slot number on a jacket card where a SPA is installed.
detail	Specifies display of additional low-level diagnostic information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(20)S2	This command was implemented on the 4-Port 10/100 Fast Ethernet SPA on the Cisco 7304 router and introduced a new address format and output.

Release	Modification
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

The output from this command is generally useful for diagnostic tasks performed by technical support.

Shared Port Adapter Usage Guidelines

The output from the **show controllers fastethernet** command for the 4-Port 10/100 Fast Ethernet SPA provides several different sections of information and statistics that are organized according to the internal hardware devices and the various paths in the flow of data on the SPA. The following sections are provided:

- Interface configuration information—Table 6 on page 182
- Media Access Control (MAC) device counters—Table 7 on page 184
- Field programmable gate array (FPGA) device counters—Table 8 on page 184
- SPA carrier card counters—Table 9 on page 185
- SPA error counters—Table 10 on page 186
- MAC destination address filtering table—Table 11 on page 187
- Virtual LAN (VLAN) filtering table—Table 12 on page 188
- Platform details (including Parallel Express Forwarding [PXF] information)—Table 13 on page 189

Several areas of the output are generally useful for diagnostic tasks performed by Cisco Systems technical support personnel only.

Examples

The following is a sample output from the **show controllers fastethernet** command on a Cisco 4500 series router:

```
Router# show controllers fastethernet 0

DEC21140 Slot 0, Subunit 0
dec21140_ds=0x60001234, registers=0x3c001000, ib=0x42301563, ring entries=256
rxring=0x40235878, rxr shadow=0x64528745, rx_head=0, rx_tail=10
txring=0x43562188, txr shadow=0x65438721, tx_head=17, tx_tail=34, tx_count=17
DEC21140 Registers
CSR0=0x23457667, CSR3=0x12349878, CSR4=0x34528745, CSR5=0x76674565
CSR6=0x76453676, CSR7=0x76456574, CSR8=0x25367648, CSR9=0x87253674
CSR11=0x23456454, CSR12=0x76564787, CSR15=0x98273465
DEC21140 PCI registers
bus_no=0, device_no=0
CFID=0x12341234, CFCS=0x76547654, CFRV=0x87658765, CFLT=0x98769876
CBIO=0x12344321, CBMA=0x23454321, CFIT=0x34567654, CFDA=0x76544567
MII registers
Register 0x00: 0x1234 0x1234 0x2345 0x3456 0x4567 0x5678 0x6789 0x7890
Register 0x08: 0x9876 0x8765 0x7654 0x6543 0x5432 0x4321 0x3210 0x2109
Register 0x10: 0x1234 0x2345 0x3456            0x4567 0x5678 0x6789 0x7890
Register 0x18: 0x9876 0x8765 0x7654 0x6543 0x5432 0x4321
DEC21140 statistics
filtered_in_sw=1000, throttled=10, enabled=10
rx_fifo_overflow=10, rx_no_enp=12, rx_late_collision=18
```

```
rx_watchdog=15, rx_process_stopped=15, rx_buffer_unavailable=1500
tx_jabber_timeout=10, tx_carrier_loss=2, tx_deffered=15
tx_no_carrier=1, tx_late_collision=10, tx_excess_coll=10
tx_process_stopped=1, fata_tx_err=0
```

The following is a sample output from the **show controllers fastethernet** command on a Cisco AS5300 router:

```
Router# show controller fastethernet 0

DEC21140
Setup Frame
 (0 ) 00e0.1e3e.c179
 (1 ) 0100.0ccc.cccc
 (2 ) 0900.2b00.000f
 (3 ) 0900.2b02.0104
 (4 ) 0300.0000.0001
 dec21140_ds=0x60BD33B8, registers=0x3C210000, ib=0x4002F75C, ring entries=32
 rxring=0x4002F844, rxr shadow=0x60F14B58, rx_head=6, rx_tail=6
 txring=0x4002FA6C, txr shadow=0x60F14BF8, tx_head=10, tx_tail=10, tx_count=0
 tx_size=32, rx_size=32
 PHY link up
 DEC21140 Registers:
 CSR0=0xFE024480, CSR3=0x4002F844, CSR4=0x4002FA6C, CSR5=0xFC660000
 CSR6=0x322C2002, CSR7=0xFFFFA241, CSR8=0xE0000000, CSR9=0xFFFDC3FF
 CSR11=0xFFFE0000, CSR12=0xFFFFFF09, CSR15=0xFFFFFEC8
 DEC21140 PCI registers:
  bus_no=2, device_no=0
  CFID=0x00091011, CFCS=0x82800005, CFRV=0x02000021, CFLT=0x0000FF00
  CBIO=0x3C210001, CBMA=0x00000000, CFIT=0x28140100, CFDA=0x00000000

 MII registers:
  Register 0x00:   0000  784D  2000  5C01  0001  0000  0000  0000
  Register 0x08:   0000  0000  0000  0000  0000  0000  0000  0000
  Register 0x10:   0000  0000  0000  0000        0000  0001  8060
  Register 0x18:   8020  0840  0000  3000  A3B9

 throttled=7, enabled=7
 rx_fifo_overflow=0, rx_no_enp=0, late_collision=0
 rx_watchdog=0, rx_process_stopped=0, rx_buffer_unavailable=0
 tx_jabber_timeout=0, tx_carrier_loss=1, tx_deferred=0
 tx_no_carrier=1, tx_late_collision=0, tx_excess_coll=0
 tx_process_stopped=0, fatal_tx_err=0
 overflow_resets=0
0 missed datagrams, 0 overruns
0 transmitter underruns, 0 excessive collisions
0 single collisions, 0 multiple collisions
0 dma memory errors, 0 CRC errors

0 alignment errors, 0 runts, 0 giants
```

The following is a sample output from the **show controllers fastethernet** command on a Cisco 7200 series router:

```
Router# show controllers fastethernet 0/0

Interface Fast Ethernet0/0
Hardware is DEC21140
 dec21140_ds=0x60895888, registers=0x3C018000, ib=0x4B019500
 rx ring entries=128, tx ring entries=128
 rxring=0x4B019640, rxr shadow=0x60895970, rx_head=0, rx_tail=0
 txring=0x4B019EC0, txr shadow=0x60895B98, tx_head=77, tx_tail=77, tx_count=0
 CSR0=0xFFFA4882, CSR3=0x4B019640, CSR4=0x4B019EC0, CSR5=0xFC660000
 CSR6=0xE20CA202, CSR7=0xFFFFA241, CSR8=0xFFFE0000, CSR9=0xFFFDD7FF
```

```
 CSR11=0xFFFE0000, CSR12=0xFFFFFF98, CSR15=0xFFFFFEC8
 DEC21140 PCI registers:
  bus_no=0, device_no=6
  CFID=0x00091011, CFCS=0x02800006, CFRV=0x02000012, CFLT=0x0000FF00
  CBIO=0x7C5AFF81, CBMA=0x48018000, CFIT=0x0000018F, CFDA=0x0000AF00
 MII registers:
  Register 0x00:   2000  780B  2000  5C00  01E1  0000  0000  0000
  Register 0x08:   0000  0000  0000  0000  0000  0000  0000  0000
  Register 0x10:   0000  0000  0000  0000        0000  0000  8040
  Register 0x18:   8000  0000  0000  3800  A3B9
 throttled=0, enabled=0, disabled=0
 rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
 tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=1
 tx_no_carrier=1, tx_late_collision=0, tx_excess_coll=0
 tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, mult_ovfl=0
HW addr filter: 0x60895FC0, ISL Enabled
  Entry= 0: Addr=0100.0CCC.CCCC
  Entry= 1: Addr=0300.0000.0001
  Entry= 2: Addr=0100.0C00.0000
  Entry= 3: Addr=FFFF.FFFF.FFFF
  Entry= 4: Addr=FFFF.FFFF.FFFF
  Entry= 5: Addr=FFFF.FFFF.FFFF
  Entry= 6: Addr=FFFF.FFFF.FFFF
  Entry= 7: Addr=FFFF.FFFF.FFFF
  Entry= 8: Addr=FFFF.FFFF.FFFF
  Entry= 9: Addr=FFFF.FFFF.FFFF
  Entry=10: Addr=FFFF.FFFF.FFFF
  Entry=11: Addr=FFFF.FFFF.FFFF
  Entry=12: Addr=FFFF.FFFF.FFFF
  Entry=13: Addr=FFFF.FFFF.FFFF
  Entry=14: Addr=FFFF.FFFF.FFFF
  Entry=15: Addr=0060.3E28.6E00
```

Shared Port Adapter Examples

The following is sample output from the **show controllers fastethernet** command for the first interface (port 0) on a 4-Port 10/100 Fast Ethernet SPA that is located in the top subslot (0), of the MSC that is installed in slot 4 on a Cisco 7304 router:

```
Router# show controllers fastethernet 4/0/0

Interface FastEthernet4/0/0
  Hardware is SPA-4FE-7304
  Connection mode is auto-negotiation
  Interface state is up, link is up
  Configuration is Auto Speed, Auto Duplex
  Selected media-type is RJ45
  Promiscuous mode is off, VLAN filtering is enabled
  MDI crossover status: MDI
  Auto-negotiation configuration and status:
    Auto-negotiation is enabled and is completed
    Speed/duplex is resolved to 100 Mbps, full duplex
    Advertised capabilities: 10M/HD 10M/FD 100M/HD 100M/FD Pause capable (Asymmetric)
    Partner capabilities: 10M/HD 10M/FD 100M/HD 100M/FD Pause capable
MAC counters:
  Input: packets = 15, bytes = 1776
         FIFO full/reset removed = 0, error drop = 0
  Output: packets = 18, bytes = 2622
          FIFO full/reset removed = 0, error drop = 0
  Total pause frames: transmitted = 0, received = 0
FPGA counters:
  Input: Total (good & bad) packets: 15, TCAM drops: 4
         Satisfy (host-backpressure) drops: 0, CRC drops: 0
         PL3 RERRs: 0
```

```
  Output: EOP (SPI4) errors: 0
SPA carrier card counters:
  Input: packets = 11, bytes = 1476, drops = 0
  Output: packets = 18, bytes = 2550, drops = 0
  Egress flow control status: XON
  Per bay counters:
  General errors: input = 0, output = 0
  SPI4 errors: ingress dip4 = 0, egress dip2 = 0
SPA Error counters:
  SPI4 TX out of frame error = 2 (00:02:31 ago)
  SPI4 TX Train valid error = 1 (00:02:11 ago)
  SPI4 TX DIP4 error = 1 (00:01:30 ago)
  SPI4 RX out of frame error = 1 (00:00:36 ago)
  SPI4 RX DIP2 error = 1 (00:00:13 ago)
MAC destination address filtering table:
  Table entries: Total = 512, Used = 4, Available = 508
  Index MAC destination address       Mask
  ----- ----------------------  --------------
  1     0007.0ed3.ba80          ffff.ffff.ffff
  2     ffff.ffff.ffff          ffff.ffff.ffff
  3     0100.0000.0000          0100.0000.0000
  4     0100.0ccc.cccc          ffff.ffff.ffff
VLAN filtering table:
  Number of VLANs configured on this interface = 0
  Table entries: Total = 1024, Used = 2, Available = 1022
  Index  VLAN identifier  Enabled  Tunnel
  -----  ---------------  -------  ------
  1           0             No      No
  2           0             Yes     No
Platform details:
  PXF tif number: 0x10
```

Table 6 describes the fields shown in the interface configuration section of the display. This section is useful for verifying the status of autonegotiation and configured parameters on the link, and the amount of traffic being handled by the interface.

Table 6 show controllers Command Field Descriptions—Interface Section

Field	Description
Interface	Name of the interface.
Hardware	Type of hardware.
Connection mode	Indicator of autonegotiation used to establish the connection.
Link	State of the link.
Configuration	Configuration of the speed and duplex operation on the interface.
Selected media-type	Interface port media type. RJ-45 is the only type supported on the 4-Port 10/100 Fast Ethernet SPA.
Promiscuous mode	State of promiscuous mode (on or off). When promiscuous mode is on, the SPA disables MAC destination address and VLAN filtering. When promiscuous mode is off, the SPA enables MAC destination address and VLAN filtering.

Table 6 show controllers Command Field Descriptions—Interface Section (continued)

Field	Description
VLAN filtering	Status of ternary content addressable memory (TCAM) filtering of VLANs (enabled or disabled). By default, the SPA always enables VLAN filtering. The SPA disables VLAN filtering if the TCAM table is full, or if the SPA is operating in promiscuous mode. **Note** VLAN filtering is not enabled or disabled using any command-line interface (CLI) command.
MDI crossover status	State of the media dependent interface (MDI) for the PHY device on the specified interface. The possible values are MDI for straight-through cables or media dependent interface crossover (MDI-X) for crossover cables.
Auto-negotiation	State of autonegotiation (enabled or disabled) on the interface and its current status.
Speed/duplex is resolved to	Results of autonegotiated parameter values (speed and duplex) currently being used on the link.
Advertised capabilities	List of the possible combinations of speed and duplex modes (in *speed/duplex* format) and flow control that the local interface has advertised it supports to the remote device: • For speed—10M is 10 Mbps, and 100M is 100 Mbps. • For duplex—HD is half duplex, and FD is full duplex. • For flow control—"Pause capable (Asymmetric)" means that the SPA advertises support of the PAUSE flow control bit and the ASM_DIR (asymmetric) flow control bit.
Partner capabilities	List of the possible combinations of speed and duplex modes (in *speed/duplex* format) and flow control that the remote device has advertised it supports to the local interface: • For speed—10M is 10 Mbps, and 100M is 100 Mbps. • For duplex—HD is half duplex, and FD is full duplex. • For flow control—"Pause capable" means that the remote device supports implementation of the PAUSE flow control bit; "Pause capable (Asymmetric)" means that the remote device supports implementation of the PAUSE flow control bit and the ASM_DIR (asymmetric) flow control bit.

Table 7 describes the fields shown in the MAC counters section of the display. This section is useful for verifying the status of packets processed by the MAC device for the interface. This information is useful for Cisco Systems technical support personnel.

Table 7 show controllers Command Field Descriptions—MAC Counters Section

Field	Description
Input: packets, bytes	Total number of packets and bytes received by the MAC device for the interface since it was activated or cleared. You can clear these counters using the **clear counters** privileged EXEC command.
Input: FIFO full/reset removed	Total number of packets removed by the MAC device due to a first-in, first-out (FIFO) overflow condition in the input buffer for the interface.
Input: error drop	Total number of input packets with errors that are dropped by the MAC device for the interface.
Output: packets, bytes	Total number of packets and bytes transmitted by the MAC device for the interface since it was activated or cleared. You can clear these counters using the **clear counters** privileged EXEC command.
Output: FIFO full/reset removed	Total number of packets removed by the MAC device due to a first-in, first-out (FIFO) overflow condition in the output buffer for the interface.
Output: error drop	Total number of output packets with errors that are dropped by the MAC device for the interface.
Total pause frames	Total number of Ethernet 802.3x pause frames transmitted and received by the MAC device for flow control on the interface.

Table 8 describes the fields shown in the FPGA counters section of the display. This section is useful for verifying the status of packets processed by the FPGA device for the interface. This information is useful for Cisco Systems technical support personnel.

Table 8 show controllers Command Field Descriptions—FPGA Counters Section

Field	Description
Input: Total (good & bad) packets	Total number of packets received by the FPGA device in the ingress direction for the interface.
Input: TCAM drops	Total number of packets dropped by the FPGA device in the ingress direction for the interface due to a ternary content addressable memory (TCAM) lookup failure. This counter increments when the interface receives a frame with a destination MAC address or VLAN identifier that is not present in the TCAM table.
Input: Satisfy (host-backpressure) drops	Total number of packets dropped by the FPGA device in the ingress direction for the interface due to back-pressure from the MSC.

Table 8 show controllers Command Field Descriptions—FPGA Counters Section (continued)

Field	Description
Input: CRC drops	Total number of packets dropped by the FPGA device in the ingress direction for the interface due to cyclic redundancy check (CRC) errors.
Input: PL3 RERRs	Total number of packets with errors received for the interface by the FPGA device in the ingress direction over the System Packet Interface Level 3 (SPI3) (also called PL3) path from the MAC device to the FPGA device.
Output: EOP (SPI4) errors	Total number of packets with end-of-packet (EOP) errors received by the FPGA device in the egress direction for the interface over the System Packet Interface Level 4 (SPI4) path from the MSC to the FPGA device.

Table 9 describes the fields shown in the SPA carrier card counters section of the display. This section is useful for verifying the status of packets processed by the MSC for the interface. This information is useful for Cisco Systems technical support personnel.

Table 9 show controllers Command Field Descriptions—SPA Carrier Card Counters Section

Field	Description
Input: packets, bytes, drops	Total number of packets, bytes, and packet drops that have occurred on the SPI4 path from the FPGA device to the MSC.
Output: packets, bytes, drops	Total number of packets, bytes, and packet drops that have occurred on the SPI4 path from the MSC to the FPGA device.
Egress flow control status	Status of flow control between the MSC and the Route Processor (RP). The possible values are: • XON—A control frame has been sent by the MSC to the RP to indicate that the MSC is ready to accept data. • XOFF—A control frame has been sent by the MSC to the RP to indicate congestion on the MSC. The MSC cannot accept any more data from the RP during this condition.
General errors	Total number of errors (such as parity) on the MSC in the ingress and egress direction.
SPI4 errors: ingress dip4	Total number of 4-bit Diagonal Interleaved Parity (DIP4) errors in the ingress direction on the SPI4 path from the FPGA device to the MSC. DIP4 is a parity algorithm where a 4-bit odd parity is computed diagonally over control and data words.
SPI4 errors: egress dip2	Total number of 2-bit Diagonal Interleaved Parity (DIP2) errors in the egress direction on the SPI4 path from the FPGA device to the MSC. DIP2 is a parity algorithm where a 2-bit odd parity is computed diagonally over status words.

Table 10 describes the fields shown in the SPA error counters section of the display. This section appears only when one of the SPI4 transmit or receive errors occurs on the interface. This information is useful for Cisco Systems technical support personnel.

Note None of the SPA SPI4 error counters appear in **show controllers fastethernet** command output until at least one of those types of SPI4 errors occurs.

All of the errors in the SPA error counters section are subject to the SPA automatic recovery process when certain thresholds are reached.

Table 10 show controllers Command Field Descriptions—SPA Error Counters Section

Field	Description
SPI4 TX out of frame error = 2 (00:02:31 ago)	Number of SPI4 out-of-frame errors (events) detected in the transmit direction (toward the network), from the MSC to the SPA FPGA device. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. This error indicates a loss of synchronization between the synchronization block and the data received on the SPI4 path. When synchronization is reacquired, the error no longer occurs.
SPI4 TX Train valid error = 1 (00:02:11 ago)	Number of times that a low-level synchronization problem was detected in the transmit direction (toward the network), from the MSC to the SPA FPGA device. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected.
SPI4 TX DIP4 error = 1 (00:01:30 ago)	Number of 4-bit Diagonal Interleaved Parity (DIP4) errors in the transmit direction (toward the network), from the MSC to the SPA FPGA device. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. DIP4 is a parity algorithm where a 4-bit odd parity is computed diagonally over control and data words.

Table 10 show controllers Command Field Descriptions—SPA Error Counters Section

Field	Description
SPI4 RX out of frame error = 1 (00:00:36 ago)	Number of SPI4 out-of-frame errors (events) detected in the receive direction (from the network), from the SPA FPGA device to the MSC. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. This error indicates a loss of synchronization between the synchronization block and the data received on the SPI4 path. When synchronization is reacquired, the error no longer occurs.
SPI4 RX DIP2 error = 1 (00:00:13 ago)	Number of 2-bit Diagonal Interleaved Parity (DIP2) errors in the receive direction (from the network), from the SPA FPGA device to the MSC. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. DIP2 is a parity algorithm where a 2-bit odd parity is computed diagonally over status words.

Table 11 describes the fields shown in the MAC destination address filtering table section of the display. This section is useful for verifying the multicast destination addresses that are in the TCAM table and permitted by the interface. This information is useful for Cisco Systems technical support personnel.

Table 11 show controllers Command Field Descriptions—MAC Destination Address Filtering Table Section

Field	Description
Table entries: Total, Used, Available	Total number of MAC destination address entries possible in the TCAM table for the interface, the number of table entries currently used by the interface, and the number of table entries that remain available. The 4-Port 10/100 Fast Ethernet SPA supports a 512-entry MAC filtering table for each supported interface (2048 entries total on the card).
Index	Table entry identifier.

Table 11 show controllers Command Field Descriptions—MAC Destination Address Filtering Table Section (continued)

Field	Description
MAC destination address	MAC destination address (multicast) permitted by the interface and used in the TCAM lookup table for packet filtering. The multicast MAC entries typically come from routing protocols [such as Open Shortest Path First (OSPF) and Enhanced IGRP (EIGRP)], and other protocols including the Hot Standby Router Protocol (HSRP). When the router reloads, three addresses appear by default in the MAC filtering table: the unicast address of the local interface, the Ethernet broadcast address, and the Ethernet multicast address.
Mask	Mask for the corresponding destination address. The SPA uses the bits that are set in the mask to look up the address in the TCAM table.

Table 12 describes the fields shown in the VLAN filtering table section of the display. This section is useful for verifying the VLANs that are in the TCAM table and are permitted by the interface. This information is useful for Cisco Systems technical support personnel.

Table 12 show controllers Command Field Descriptions—VLAN Filtering Table Section

Field	Description
Number of VLANs configured on this interface	Number of VLANs that are configured on the interface. If the number of VLANs configured on the interface is 1022 or less, then the VLAN filtering table also shows an index entry for every VLAN ID. The number of VLANs configured on the interface can be 0, while the number of used table entries reports 2, because the SPA always uses two entries to provide valid matching criteria for promiscuous mode and non-VLAN packets.
Table entries: Total, Used, Available	Total number of VLAN entries possible in the TCAM filtering table for the interface, the number of table entries currently used by the interface (two are always in use by default), and the number of table entries that remain available. The 4-Port 10/100 Fast Ethernet SPA supports a 1024-entry VLAN filtering table for each supported interface (4096 entries total on the card).
Index	Table entry identifier.
VLAN identifier	Number of the VLAN. Two VLAN ID 0 entries always appear in the table and represent the local interface port for handling of promiscuous mode and non-VLAN packets. Other VLAN entries appear in this table when VLANs are configured on the interface.

Table 12 show controllers Command Field Descriptions—VLAN Filtering Table Section

Field	Description
Enabled	Status of the VLAN ID for TCAM filtering, with the following possible values: • No—The entry is disabled for filtering. • Yes—The entry is enabled for filtering. The TCAM filter uses the "first-match" rule to filter packets that the SPA receives against entries in the table. The matching assessment begins at the top of the table with the VLAN ID 0 entries. **Note** The SPA always supports two VLAN ID 0 entries. The first VLAN ID 0 entry of the TCAM table is used for promiscuous mode. It has a value of "No," meaning it is disabled, whenever promiscuous mode is disabled for the interface. The second VLAN ID 0 entry is used for filtering of non-VLAN packets.
Tunnel	Status of tunneling for the interface, with the following possible values: • No—Tunneling is disabled and the SPA performs MAC destination address filtering. • Yes—Tunneling is enabled and the SPA does not perform MAC destination address filtering. **Note** If promiscuous mode is enabled, then the first VLAN ID 0 entry shows tunnel = Yes. All other VLAN ID entries show tunnel = No.

Table 13 describes the fields shown in the Platform details section of the display.

Table 13 show controllers Command Field Descriptions—Platform Details Section

Field	Description
PXF tif number	Number of the interface (in hexadecimal format) used for PXF on the network services engine (NSE) or by the Hyper Transport (HT) FPGA device on the network processing engine (NPE).

Related Commands

Command	Description
show interfaces fastethernet	Displays information about the Fast Ethernet interfaces.

show cwan

To display the WAN statistics and information about the hidden VLAN-to-WAN interface, use the **show cwan** command in user EXEC mode.

show cwan {**stats** | **vlans**}

Syntax Description

stats	Displays information about the WAN statistics.
vlans	Displays the hidden VLAN-to-WAN interface mapping.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
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 720.

The **show vlan internal usage** command displays the internal VLANs that are allocated to WAN interfaces as Layer 3 VLANs but does not display the associated subinterfaces. To display the associated subinterfaces, enter the **show cwan vlans** command. The **show cwan vlans** command displays the mapping between the WAN subinterface and the internal VLANs in use.

Examples

This example shows how to display the information about the WAN port statistics:

```
Router# show cwan stats

0 unknown VLANs
0 ATM packets with zero src_ltl or inactive VC
0 unknown enctype
0 output unknown enctype drops
0 particle alloc failures
0 pak alloc failures
Router#
```

This example shows how to display the hidden VLAN-to-WAN interface mappings:

```
Router# show cwan vlans

Hidden VLAN swidb->if_number Interface
-----------------------------------------------
1017 75 ATM2/0/0
1018 90 ATM2/0/0.54
1019 92 ATM2/0/0.56
```

```
1020 93 ATM2/0/0.57
1021 94 ATM2/0/0.100
1022 95 ATM2/0/0.101
1023 96 ATM2/0/0.102
1024 97 ATM2/0/0.103
1025 98 ATM2/0/0.110
1026 99 ATM2/0/0.111
1027 100 ATM2/0/0.112
1028 101 ATM2/0/0.113
1029 102 ATM2/0/0.120
1030 103 ATM2/0/0.200
1031 104 ATM2/0/0.201
1032 105 ATM2/0/0.202
1033 106 ATM2/0/0.203
1067 76 POS4/1
1068 77 POS4/2
1071 79 GE-WAN5/2
1072 80 GE-WAN5/3
1073 81 GE-WAN5/4
Recycled VLAN Interface
-----------------------------
Pending recycle holdtime(ms) Interface
-----------------------------------------
Router#
```

Related Commands

Command	Description
ip access-list hardware permit fragments	Permits all noninitial fragments in the hardware.

show cwan qinq

To display the inner, outer, and trunk VLANs that are used in IEEE 802.1Q-in-802.1Q (QinQ) translation, use the **show cwan qinq** command in privileged EXEC mode.

show cwan qinq [**configured** | **detail** | **list**]

Syntax Description

configured	(Optional) Displays statistics for all configured bridge domains.
detail	(Optional) Displays the details of the inner VLAN configurations for each bridge domains.
list	(Optional) Displays the currently configured assignments.

Command Default

The inner, outer, and trunk VLANs that are used in IEEE 802.1Q-in-802.1Q (QinQ) translation are not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed as follows: • Support was added for QinQ link bundles that use virtual port-channel interfaces. • The **configured**, **detail**, and **list** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is supported on the Gigabit Ethernet 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.

The **show cwan qinq** command shows a summary of the QinQ translations being performed. See the other related commands for additional information:

- **show cwan qinq**
- **show cwan qinq bridge-domain**
- **show cwan qinq interface**

Examples

This example shows the typical output from the **show cwan qinq** command:

```
Router# show cwan qinq

Bridge-domain   Interface       Egress-if       Inner-start Total Active
32              GE4/4           GE4/4           32          1     1
  Sub-Interface   Trunk-vlan   Inner-vlan   Service         State
  GE4/4.1         101          32           dot1q           up/down

Bridge-domain   Interface       Egress-if       Inner-start Total Active
888             Po1             GE4/1           32          1     1
  Sub-Interface   Trunk-vlan   Inner-vlan   Service         State
  Po1.1           101          32           dot1q           up/up

Router#
```

Table 14 describes the fields shown in the display.

Table 14 show cwan qinq Field Descriptions

Field	Description
Bridge-domain	VLAN ID for the outer PE VLAN tag that is expected on the original incoming packets.
Interface	Gigabit Ethernet WAN interface or subinterface being used for the QinQ translation.
Egress-if	Output interface being used for packets on this particular subinterface and PE VLAN ID.
Inner-start	Start of the 32-count block of inner CE VLAN IDs that are being used for the outer PE VLAN tag. The base number is always evenly divisible by 32. Any CE VLAN IDs that do not fall within this block of 32 IDs are considered to be out of range.
Total	Total number of CE VLAN subinterfaces that are configured for this PE VLAN ID (bridge domain).
Active	Total number of VLAN translations that are currently active for this bridge domain.
Sub-interface	Subinterface on a Gigabit Ethernet WAN interface or port-channel interface for this particular VLAN translation.
Trunk-vlan	VLAN ID for the trunk VLAN tag that is added to the outgoing translated packet as the outer (or only) VLAN tag.
Inner-vlan	VLAN ID for the inner CE VLAN tag that is expected on the original incoming packets.

Table 14 show cwan qinq Field Descriptions (continued)

Field	Description
Service	Type of QinQ configuration being used on the subinterface: • **dot1q-drop**—Invalid configuration or all packets are being dropped. • **dot1q**—Subinterface is configured for QinQ translate mode (two-tags to one-tag translation: **bridge-domain dot1q**). • **dot1q-tunnel**—Subinterface is configured for QinQ tunnel mode (two-tags to two-tags transparent tunneling: **bridge-domain dot1q-tunnel**). • **dot1q-tunnel out-range**—Subinterface is configured for out-of-range packets for this particular PE VLAN (**bridge-domain dot1q-tunnel out-range**).
State	Current

Related Commands

Command	Description
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
mode dot1q-in-dot1q access-gateway	Enables a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation.
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 QinQ-translated outgoing packet with the priority value from the inner customer-edge VLAN tag.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

show cwan qinq bridge-domain

To display the provider-edge VLAN IDs that are used on a Gigabit Ethernet WAN interface for 802.1Q in 802.1Q (QinQ) translation or to show the customer-edge VLANs that are used for a specific provider-edge VLAN, use the **show cwan qinq bridge-domain** command in privileged EXEC mode.

show cwan qinq bridge-domain [*pe-vlan-id*]

Syntax Description

pe-vlan-id	(Optional) Information for the specified provider-edge VLAN ID; valid values are from 1 to 4094.

Command Default

If you do not specify a *vlan-id*, the provider-edge VLANs that are configured for each Gigabit Ethernet WAN interface displays.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced as **show cwan qinq bridge-vlan** on the Supervisor Engine 720.
12.2(18)SXE	This command was renamed **show cwan qinq bridge-domain**. Support was also added for QinQ link bundles using port-channel virtual 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 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.

Examples

This example shows typical output from the **show cwan qinq bridge-domain** command. This output displays the provider-edge VLANs (bridge VLANs) for all GE-WAN interfaces on the Catalyst 6500 series switch:

```
Router# show cwan qinq bridge-domain

GE-WAN5/1, group 1, total_rate 2
 2, 4062
GE-WAN5/2, group 1, total_rate 1
 150
GE-WAN5/3, group 1, total_rate 2
 100, 1000
GE-WAN5/4, group 1, total_rate 16
 3-5, 7-10,12-15,18-20,22, 4094
Port-channel1, group 1, total_rate 21

Router#
```

This example shows typical output for a specific provider-edge VLAN:

```
Router# show cwan qinq bridge-domain 4094

Bridge-domain   Interface       Egress-if       Inner-start Service Count
4093            GE5/4             GE2/3           192         31
  Sub-Interface   Trunk-vlan   Inner-vlan   Service
  GE5/4.4000      4000         default      dot1q-tunnel out-ran
  GE5/4.4062      4062         1            dot1q-tunnel
  GE5/4.4064      4064         3            dot1q-tunnel
  GE5/4.4067      4067         6            dot1q-tunnel
  GE5/4.4068      4068         7            dot1q-tunnel

.
.
.
```

Table 15 describes the fields shown in the display.

Table 15 show cwan qinq bridge-domain Field Descriptions

Field	Description
Bridge-domain	Outer provider-edge VLAN IDs that are configured on the subinterfaces for this interface. These IDs are shown as a range, where possible, or as individual IDs.
interface	Gigabit Ethernet WAN interface or subinterface that is used.
Egress-if	Output interface being used for packets on this particular subinterface and VLAN.
Inner-start	Start of the 32-count block of inner customer-edge VLAN IDs that are used for the outer provider-edge VLAN tag. The base number is always evenly divisible by 32. Any customer-edge VLAN IDs that do not fall within this block of 32 IDs are out of range.
Service Count	Number of service translations that are currently configured and in use.
Tr-vlan	VLAN ID for the trunk VLAN tag that is added to the outgoing translated packet as the outer (or only) VLAN tag.
Inner-vlan	VLAN ID for the inner customer-edge VLAN tag that is expected on the original packets received on this subinterface. If this field shows “default,” it indicates that the subinterface matches all out-of-range packets (packets with a customer-edge VLAN ID that are not within the configured 32-count block of customer-edge VLAN IDs).
Service	Type of QinQ configuration that is used on the subinterface: • **dot1q-drop**—Invalid configuration or all packets are being dropped. • **dot1q**—Subinterface is configured for QinQ translate mode (two-tags to one-tag translation: **bridge-vlan dot1q**). • **dot1q-tunnel**—Subinterface is configured for QinQ tunnel mode (two-tags to two-tags transparent tunneling: **bridge-vlan dot1q-tunnel**). • **dot1q-tunnel out-ran**—Subinterface is configured for out-of-range packets for this particular provider-edge VLAN (**bridge-vlan dot1q-tunnel out-range**).

Related Commands

Command	Description
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
mode dot1q-in-dot1q access-gateway	Enables a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation.
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 QinQ-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 QinQ translation.
show cwan qinq interface	Displays interface statistics for IEEE 802.1Q-in-802.1Q (QinQ) translation on one or all Gigabit Ethernet WAN interfaces and port-channel interfaces.

show cwan qinq interface

To display interface statistics for IEEE 802.1Q-in-802.1Q (QinQ) translation on one or all Gigabit Ethernet WAN interfaces and port-channel interfaces, use the **show cwan qinq interface** command in privileged EXEC mode.

show cwan qinq interface [**gigabitethernet** [*slot*/*port*[**.***subint*]] | **port-channel** *channel-number* [**.***subint*]]

Syntax Description

gigabitethernet *slot*/*port*	(Optional) Specifies the Gigabit Ethernet WAN interface to be displayed.
port-channel *channel-number*	(Optional) Specifies a port-channel virtual interface to be displayed; valid values are from 1 to 282.
.*subint*	(Optional) Subinterface number to be displayed. The period (**.**) is required.

Command Default

If you enter this command without any arguments, it displays information for all the Gigabit Ethernet WAN interfaces in the Catalyst 6500 series switch.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to add the **port-channel** keyword to support QinQ link bundles that use port-channel virtual 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 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.

The valid range for user-created port-channel numbers is from 1 to 256. Channel numbers 257 to 282 are system-created channels that are used internally, and their statistics are typically useful only for help in troubleshooting and debugging.

The **show cwan qinq interface** command displays the same interface counters that are shown by the **show interfaces** command but displays them by subinterface with the associated QinQ provider-edge and customer-edge VLANs.

Examples

This example shows the output from the **show cwan qinq interface** command:

```
Router# show cwan qinq interface

Interface        Status    Egress op PE   CE   TRNK Input packets/       Output packets/
                                                    Input bytes          Output bytes
---------------- --------- ------ -- ---- ---- ---- -------------------- ----------------
GE1/2.500        up        GE3/3  1  50   3200 500  0                    0
                                                    0                    0
GE1/2.501        up        GE3/3  1  50   3201 501  3586                 3498
                                                    466294               412323
GE1/2.502        up        GE3/3  1  50   3202 502  3577                 3481
                                                    464844               410704
.
.
.
Router#
```

This example shows the output for a specific interface:

```
Router# show cwan qinq interface GE-WAN 1/2

Interface        Status    Egress op PE   CE   TRNK Input packets/       Output packets/
                                                    Input bytes          Output bytes
---------------- --------- ------ -- ---- ---- ---- -------------------- ----------------
GE1/2.500        up        GE7/0  1  50   3200 500  626485               63571
                                                    492579036            508305780
GE1/2.501        up        GE7/0  1  50   3201 501  626483               63571
                                                    492579644            508305780
GE1/2.502        up        GE7/0  1  50   3202 502  626485               63571
                                                    492701011            508305780
.
.
.
Router#
```

This example shows the output for a specific subinterface:

```
Router# show cwan qinq interface GE-WAN 5/1.1000

Interface        Status    Egress op PE   CE   TRNK Input packets/       Output packets/
                                                    Input bytes          Output bytes
---------------- --------- ------ -- ---- ---- ---- -------------------- ----------------
GE5/1.1000       up        GE3/1  1  2    2496 1000 476790463            12108753
                                                    47168162431          1110048768
Router#
```

This example shows an excerpt from the typical output for a specific subinterface:

```
Router# show cwan qinq interface GE-WAN 5/1.1000

Interface        Status    Egress op PE   CE   TRNK Input packets/       Output packets/
                                                    Input bytes          Output bytes
---------------- --------- ------ -- ---- ---- ---- -------------------- ----------------
GE5/1.1000       up        GE3/1  1  2    2496 1000 476790463            12108753
                                                    47168162431          1110048768

Router#
```

This example shows an excerpt from the typical output for a specific port-channel virtual interface:

```
Router# show cwan qinq interface port 3

Interface        Status    Egress op PE   CE   TRNK Input packets/       Output packets/
                                                   Input bytes           Output bytes
---------------- --------- ------ -- ---- ---- ---- -------------------- ----------------
Po3.101          up/up     GE2/3  1  150  223  323  59759000             23971
                                                   3824576384           819613
Po3.102          up/up     GE2/3  1  150  222  324  59758987             23914
                                                   3824575552           818231
.
.
.
Router#
```

Table 16 describes the fields shown in the displays.

Table 16 show cwan qinq interface Field Descriptions

Field	Description
Interface	Gigabit Ethernet WAN or port-channel interface or subinterface being used.
Status	Current status of this interface: up or down.
Egress	Output interface being used for packets on this particular subinterface and VLAN.
op	Operational status code and QinQ configuration of this subinterface: • 0—Invalid configuration or all packets are being dropped. • 1—Subinterface is configured for QinQ translate mode (two-tags to one-tag translation: **bridge-domain dot1q**). • 2—Subinterface is configured for QinQ tunnel mode (two-tags to two-tags transparent tunneling: **bridge-domain dot1q-tunnel**). • 3—Not used. • 4—Subinterface is configured for out-of-range packets for this particular PE VLAN (**bridge-domain dot1q-tunnel out-range**).
PE	Outer provider edge (PE) VLAN IDs that have been configured on the subinterfaces for this interface.
CE	VLAN ID for the inner customer edge (CE) VLAN tag that is expected on the original packets being received on this subinterface.
Trnk	VLAN ID for the trunk VLAN tag that is added to the outgoing translated packet as the outer (or only) VLAN tag.
Input packets	Number of packets received on this subinterface.
Input bytes	Number of bytes received on this subinterface.
Output packets	Number of translated packets that were transmitted out this subinterface.
Output bytes	Number of translated bytes that were transmitted out this subinterface.

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.
mode dot1q-in-dot1q access-gateway	Enables a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation.
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 QinQ-translated outgoing packet with the priority value from the inner customer-edge VLAN tag.
show cwtlc qinq	Displays the information that is related to QinQ translation and is contained in the XCM on board the supervisor engine.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

show cwan qinq load-balance

To display load-balancing statistics for IEEE 802.1Q-in-802.1Q (QinQ) translation on one or all Gigabit Ethernet WAN interfaces and port-channel interfaces, use the **show cwan qinq load-balance** command in privileged EXEC mode.

show cwan qinq load-balance [*channel-number* | **configured** | **detail** | **list**]

Syntax Description

channel-number	(Optional) Statistics for a specific channel group; valid values are from 1 to 256.
configured	(Optional) Displays statistics for all configured port channels.
detail	(Optional) Displays the details of the inner VLAN configurations for each port channel.
list	(Optional) Displays the currently configured assignments.

Command Default

If you enter this command without any options, it displays information for all Gigabit Ethernet WAN and port-channel interfaces in the router.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE	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.

Examples

This example shows an excerpt from the typical output from the default form of the **show cwan qinq load-balance** command:

```
Router# show cwan qinq load-balance

Port-channel10 total 505 bridge-domain vlan(s) active
  Po10 - GE-WAN3/1 has 167 bridge-domain vlan(s) active
  Po10 - GE-WAN3/2 has 169 bridge-domain vlan(s) active
  Po10 - GE-WAN9/1 has 169 bridge-domain vlan(s) active

  Port-channel20 total 4 bridge-domain vlan(s) active
  Po20 - GE-WAN3/3 has 1 bridge-domain vlan(s) active
  Po20 - GE-WAN3/4 has 1 bridge-domain vlan(s) active
  Po20 - GE-WAN9/2 has 1 bridge-domain vlan(s) active
  Po20 - GE-WAN9/3 has 1 bridge-domain vlan(s) active

Router#
```

This example shows typical output when using the **configured** keyword:

```
Router# show cwan qinq load-balance configured

 Port-channel1 total 1 bridge-domain vlan(s) active
   Po1 - GE-WAN4/1 has 1 bridge-domain vlan(s) active
```

```
        GE-WAN4/1 has 1 bridge-domain vlan(s) configured: 888
  Po1 - GE-WAN8/1 has 0 bridge-domain vlan(s) active
        GE-WAN8/1 has 1 bridge-domain vlan(s) configured: 889

Router#
```

This example shows typical output when using the **list** keyword:

```
Router# show cwan qinq load-balance list

 Port-channel1 total 1 bridge-domain vlan(s) active
   Po1 - GE-WAN4/1 has 1 bridge-domain vlan(s) active
   Po1 - GE-WAN4/1 active vlan(s): 888

   Po1 - GE-WAN8/1 has 0 bridge-domain vlan(s) active
   Po1 - GE-WAN8/1 active vlan(s): 889

Router#
```

This example shows typical output when using the **detail** keyword:

```
Router# show cwan qinq load-balance detail

 Port-channel1 total 1 bridge-domain vlan(s) active
   Po1 - GE-WAN4/1 has 1 bridge-domain vlan(s) active
     Bridge-domain Inner  Configured Active
     ------------- ------ ---------- ------
     888           active 3          2
   Po1 - GE-WAN8/1 has 0 bridge-domain vlan(s) active
     Bridge-domain Inner  Configured Active
     ------------- ------ ---------- ------
     889           -      1          0

Router#
```

Table 17 describes the fields shown in this display.

Table 17 show cwan qinq load-balance detail Field Descriptions

Field	Description
Bridge-domain	PE VLANs being used on this interface.
Inner	Number of inner VLANs configured for this bridge domain.
Configured	Number of bridge domains that are configured on this interface.
Active	Number of bridge domains that are configured and active on this interface.

Related Commands

Command	Description
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
mode dot1q-in-dot1q access-gateway	Enables a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation.
policy-map	Accesses QoS policy-map configuration mode to configure the QoS policy map.
service-policy	Attaches a policy map to an interface.

Command	Description
set cos cos-inner (policy-map configuration)	Sets the 802.1Q prioritization bits in the trunk VLAN tag of a QinQ-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 QinQ translation.
show cwan qinq interface	Displays interface statistics for IEEE QinQ translation on one or all Gigabit Ethernet WAN interfaces and port-channel interfaces.

show cwan qinq port-channel

To display IEEE 802.1Q-in-802.1Q (QinQ) statistics for one or all configured QinQ link bundles (port channels), use the **show cwan qinq port-channel** command in privileged EXEC mode.

show cwan qinq port-channel [**detail** *channel-number*]

Syntax Description

detail *channel-number*	(Optional) Displays statistics for a specific port-channel group; valid values are from 1 to 256.

Command Default

If you use this command without the **detail** keyword, it displays statistics for all configured QinQ link bundles.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE	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 displays the QinQ-related information for one or all port-channel groups that are being used for QinQ link bundles.

Note To display interface statistics, use the **show cwan qinq interface** command.

Examples

This example shows an excerpt from the typical output from the default form of the **show cwan qinq port-channel** command:

```
Router# show cwan qinq port-channel

Group    : WAN          if_num idb      pagp         if_num idb      port
---------  ------------ d----- x------- ------------ d----- x------- d--
Group 1  : GE-WAN9/1    67     43CABB20 GE-WAN 9/1   88     4529B710 5

Router#
```

Table 18 describes the fields shown in the display.

Table 18 show cwan qinq port-channel Field Descriptions

Field	Description
Group	Channel group to which this interface belongs.
WAN	Interface being displayed.

Table 18 show cwan qinq port-channel Field Descriptions (continued)

Field	Description
if_num	Internal number for this interface.
idb	Memory value (in hexadecimal) for this interface in the interface database.
pagp	Interface providing the port aggregation protocol (PAGP) support.
if_num	Internal number for the PAGP interface.
idb	Memory value (in hexadecimal) for the PAGP interface in the interface database.
port	Port number.

show cwtlc qinq

To display the information that is related to IEEE 802.1Q-in-802.1Q (QinQ) translation and is contained in the XCM onboard the supervisor engine, use the **show cwtlc qinq** command in privileged EXEC mode.

show cwtlc qinq *port* [**outer-vlan** *vlan-id* [*inner-vlan-id*] | **trunk-vlan** *vlan-id*]

show cwtlc qinq qos

Syntax Description

port	Port number for the information to be displayed; valid values are from 0 to 3.
outer-vlan *vlan-id*	(Optional) Displays the XCM tables for a specific outer provider-edge VLAN ID; valid values are from 1 to 4094.
inner-vlan-id	(Optional) XCM tables for a specific inner customer-edge VLAN ID; valid values are from 1 to 4094.
trunk-vlan *vlan-id*	(Optional) Displays the XCM tables for a specific trunk VLAN ID that is put on translated packets as the new outer VLAN tag; valid values are from 1 to 4094.
qos	Displays the source of the 802.1P bits that are being inserted into the outer trunk VLAN tag of translated packets.

Command Default

If you do not specify a specific VLAN ID, the command displays information for all VLANs.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXD	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 supported on the Gigabit Ethernet 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.

Examples

This example shows the output for a specific combination of provider-edge and customer-edge VLAN IDs:

```
Router# show cwtlc qinq 0 outer-vlan 20 21

TX VLAN FUNC TABLE
func 4, ce vlan base 0, value 4

TX VLAN TABLE
tx vlan status 1
```

```
TX ADJ TABLE
ce_vlan_offset trunk_vlan op_code src_ltl def_fn  pbit intfid
15             2          1       120     2       1    2

Router#
```

This example shows the output for the **trunk-vlan** keyword:

```
Router# show cwtlc qinq 0 trunk-vlan 2

RX VLAN FUNC TABLE
rx_vlan_func 2

RX TVC TABLE
rx_tvc_func src_ltl pe_vlan ce_vlan Q intfid
1           E0      1       20      0 2

Router#
```

Table 19 describes the fields shown in the display.

Table 19 show cwtlc qinq Command Field Descriptions

Field	Description
TX VLAN FUNC TABLE	
ce vlan base	Start of the 32-count block of inner customer-edge VLAN IDs that are used for the outer provider-edge VLAN tag. The base number is always evenly divisible by 32. Any customer-edge VLAN IDs that do not fall within this block of 32 IDs are out of range.
TX VLAN TABLE	
tx vlan status	Transmit VLAN Status: • 0—QINQ_TX_DEF_DROP: Packet dropped. • 1—QINQ_TX_DEF_TRANSPARENT: Transparent tunneling.
TX ADJ TABLE	
trunk_vlan	VLAN ID for the trunk VLAN tag that is added to the outgoing translated packet as the outer (or only) VLAN tag.
op_code	Operational status and QinQ configuration of this subinterface: • 0—Invalid configuration or all packets are being dropped. • 1—Subinterface is configured for QinQ translate mode (two-tags to one-tag translation: **bridge-vlan dot1q**). • 2—Subinterface is configured for QinQ tunnel mode (two-tags to two-tags transparent tunneling: **bridge-vlan dot1q-tunnel**). • 3—Not used. • 4—Subinterface is configured for out-of-range packets for this particular provider-edge VLAN (**bridge-vlan dot1q-tunnel out-range**).
src_ltl	Source local target logic (LTL) address for this entry.

Table 19 show cwtlc qinq Command Field Descriptions (continued)

Field	Description
use_ce_pbit	Status of whether the outgoing translated packet is using the 802.1P bits (P bits) that are copied from the original packet's outer provider-edge VLAN tag or from the original packet's inner customer-edge VLAN tag: • 0 = P bits are copied from the outer provider-edge VLAN tag. • 1 = P bits are copied from the inner customer-edge VLAN tag. See the **set cos cos-inner (policy-map configuration)** command.
intfid	Interface ID for the Gigabit Ethernet WAN interface that is used for the QinQ translation.
RX VLAN FUNC TABLE	
rx_vlan_func	Last performed function: • 0—RXVLAN_DROP: Packet was dropped • 1—RXVLAN_NORMAL: Normal Ethernet packet • 2—RXVLAN_GATEWAY: Received packet from QinQ access gateway • 3—RXVLAN_L2_LISTEN • 4—RXVLAN_L2_LEARN • 5—RXVLAN_QINQ_FORWARD • 6—RXVLAN_WAN_TRUNK—Trunk VlAN
RX TVC TABLE	
rx_tvc_func	Last performed function: • 0—DROP: Packet was dropped • 1—GATEWAY_TRANSLATE: QinQ translation (double-tag to single-tag translation) • 2—GATEWAY_TRANSPARENT: QinQ transparent tunneling (double-tag to double-tag translation) • 3—WANTRUNK_XCONNECT: WAN port cross-connect • 4—WANTRUNK_SWITCH: WAN port switching
src_ltl	Source local target logic (LTL) address for this entry.
pe_vlan	Provider-edge VLAN ID.
ce_vlan	Customer-edge VLAN ID.
intfid	Interface ID for the Gigabit Ethernet WAN interface that is used for the QinQ translation.

Related Commands

Command	Description
bridge-vlan	Maps a subinterface to specific inner customer-edge and outer provider-edge VLAN tags using QinQ translation.
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
mode dot1q-in-dot1q access-gateway	Enables a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation.
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 QinQ-translated outgoing packet with the priority value from the inner customer-edge VLAN tag.
show cwtlc qinq	Displays the information that is related to QinQ translation and is contained in the XCM on board the supervisor engine.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

show dot1q-tunnel

To display a list of 802.1Q tunnel-enabled ports, use the **show dot1q-tunnel** command in user EXEC mode.

show dot1q-tunnel [**interface** *interface interface-number*]

Syntax Description

interface *interface*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel**, and **ge-wan**.
interface-number	(Optional) Interface number; see the "Usage Guidelines" section for valid values.

Command Modes

User EXEC (>)

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.

Usage Guidelines

If you do not enter any keywords, the 802.1Q tunnel ports for all interfaces are displayed.

The **ge-wan** keyword is not supported in Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The *interface-number* argument designates the module and port number for the **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, and **ge-wan** keywords. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

The *interface-number* argument designates the port-channel number for the **port-channel** keyword; valid values are from 1 to 282. The values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

Examples

This example indicates that the port is up and has one 802.1Q tunnel that is configured on it. The fields shown in the display are self-explanatory.

```
Router# show dot1q-tunnel interface port-channel 10

Interface
---------
Po10
```

Related Commands

Command	Description
switchport mode	Sets the interface type.
vlan dot1q tag native	Enables dot1q tagging for all VLANs in a trunk.

show errdisable flap-values

To display conditions that cause a flap error to be recognized as a result of a specific cause, use the **show errdisable flap-values** command in user EXEC or privileged EXEC mode.

show errdisable flap-values

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)	This command was introduced in a release earlier than Cisco IOS Release 15.0(1) on the Cisco 3845 series routers.

Usage Guidelines

The Flaps column in the display shows how many changes to the state within the specified time interval will cause an error to be detected and a port to be disabled. For example, the display in the "Examples" section shows that an error will be assumed and the port shut down if three Dynamic Trunking Protocol (DTP)-state (port mode access/trunk) or Port Aggregation Protocol (PAgP) flap changes occur during a 30-second interval, or if 5 link-state (link up/down) changes occur during a 10-second interval.

Examples

The following is sample output from the **show errdisable flap-values** command:

```
Router# show errdisable flap-values

ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3       30
dtp-flap               3       30
link-flap              20      10
```

Table 20 describes the significant fields shown in the display.

Table 20 show errdisable flap-values Field Descriptions

Field	Description
ErrDisable Reason	Reason for error disable.
Flaps	Total number of flaps.
Time (sec)	Time set for the recovery timer, in seconds.
pagp-flap	PAgP flap error disable.
dtp-flap	DTP flap error disable.
link-flap	Link flap error disable.

Related Commands

Command	Description
errdisable detect cause	Enables the error-disabled detection for a specific cause or all causes.
errdisable recovery	Configures the recovery mechanism variables.

show gvrp interface

To display Generic VLAN Registration (GVRP) interface states, use the **show gvrp interface** command in privileged EXEC mode.

show gvrp interface

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to obtain GVRP interface detals of the administrative and operational GVRP states of all or one particular .1Q trunk port in the device.

Examples

The following example shows sample summary output:

```
Router# show gvrp interface

Port      Status    Mode            Registrar State
Fa3/1     on        slow compact    normal
Gi6/13    on        fast compact    normal
Gi6/14    on        fast compact    normal

Port      Transmit Timeout   Leave Timeout   Leaveall Timeout
Fa3/1     200                600             10000
Gi6/13    200                600             10000
Gi6/14    200                600             10000

Port      Vlans Declared
Fa3/1     1,1200,4000,4094
Gi6/13    2-40,100,200,1200,4000,4094
Gi6/14    1200,4000,4094

Port      Vlans Registered
Fa3/1     1-40,100,200
Gi6/13    1,10
Gi6/14    1-40,100,200

Port      Vlans Registered and in Spanning Tree Forwarding State
Fa3/1     1
Gi6/13    10
Gi6/14    none
```

Related Commands

Command	Description
show gvrp summary	Displays the GVRP configuration at the device leve.

show gvrp summary

To display the Generic VLAN Registration Protocol (GVRP) configuration, use the **show gvrp summary** command in privileged EXEC mode.

show gvrp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to obtain GVRP VLAN configuration details.

Examples

The following example shows sample summary output. The fields shown in the display are self-explanatory.

```
Router# show gvrp summary

GVRP global state           : enabled
GVRP VLAN creation          : disabled
VLANs created via GVRP      : 41-99, 1201-4094
```

Related Commands

Command	Description
show gvrp interface	Displays details of the adminstrative and operational GVRP states of all or one particular .1Q trunk port in the device.

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** *mac-addr*] [**interface** *type/number*] [**fa | gi** *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*] | [**count** [**module** *number* | **vlan** *vlan-id*]] | [**interface** *type/number*] | [**limit** [**vlan** *vlan-id* | **module** *number* | **interface** *interface-type*]] | [**module** *number*] | [**multicast** [**count** | {**igmp-snooping | mld-snooping** [**count**] | **user** [**count**] | **vlan** *vlan-id*}]] | [**notification** {**mac-move** [**counter** [*vlan*] | **threshold | change**} [**interface** [*interface-number*]]] | [**synchronize statistics**] | [**unicast-flood**] | **vlan** *vlan-id* [**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 Fast Ethernet.
gi	(Optional) Specifies Gigabit Ethernet.
slot/port	(Optional) Adds dynamic addresses to the module in slot 1 or 2. The **/** 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 **/** 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.
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	The **self**, **aging-time**, **count**, and **vlan** *vlan-id* keywords and arguments were added.
11.2(8)SA5	The **atm** *slot/port* keyword and arguments were added.
12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.1(8a)EW	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 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 the Supervisor Engine 720.

Release	Modification
12.2(17a)SX	For the Catalyst 6500 and 6000 series switches and 7600 series, this command was changed to support the following optional keywords and arguments: • **unicast-flood** • **count module** *number* • **limit** [**vlan** *vlan-id* | **port** *number* | **interface** *interface-type*] • **notification threshold**
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	For the Catalyst 6500 and 6000 series switches and 7600 series, this command was changed to support the **mld-snooping** keyword on the Supervisor Engine 720 only.
12.2(18)SXF	For the Catalyst 6500 and 6000 series switches and 7600 series, this command was changed to support the **synchronize statistics** keywords on the Supervisor Engine 720 only.
12.2(33)SRA	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	The **change** keyword was added.
12.2(33)SXI	This command was changed to add the **counter** keyword.

Usage Guidelines

Cisco 2600, 3600, and 3700 Series Routers

This 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 6500 and 6000 Series Switches and 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 and argument are supported only on DFC modules. The **module** *number* keyword and argument 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

Cisco 2600, 3600, and 3700 Series Routers

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

```
Router# 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
```

Catalyst 4500 Series Switches

This 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
Switch#
```

This 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
Switch#
```

Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

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.

This example shows how to display the information about the MAC address table for a specific MAC address with a Supervisor Engine 720:

```
Router# 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
```

This 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
```

This example shows how to display the currently configured aging time for all VLANs:

```
Router# show mac-address-table aging-time

Vlan    Aging Time
----    ----------
*100     300
200     1000
```

This example shows how to display the entry count for a specific slot:

```
Router# 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
```

This example shows how to display the information about the MAC address table for a specific interface with a Supervisor Engine 720:

```
Router# 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.

This example shows how to display the limit information for a specific slot:

```
Router# 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:

```
Router# show mac-address-table notification mac-move

MAC Move Notification: Enabled
Router#
```

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
```

This example shows how to display the CAM-table utilization-notification status:

```
Router# show mac-address-table notification threshold

Status limit Interval
-------------+-----------+-------------
enabled 1 120
```

This example shows how to display the MAC notification parameters and history table:

```
Router# 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
--------------------         -------------- ----------------
```

This example shows how to display the MAC notification parameters and history table for a specific interface:

```
Router# 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
```

This example shows how to display unicast-flood information:

```
Router# 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
```

This example shows how to display the information about the MAC-address table for a specific VLAN:

```
Router# 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
```

This example shows how to display the information about the MAC address table for MLDv2 snooping:

```
Router# 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
```

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 static MAC address table entries only.

show mac-address-table aging-time

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

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

show mac-address-table aging-time

Catalyst Switches

show mac-address-table aging-time [**vlan** *vlan-id*] [[**begin** | **exclude** | **include**] *expression*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; valid values are from 1 to 1005.
begin	(Optional) Specifies that the output display begin with the line that matches the *expression*.
exclude	(Optional) Specifies that the output display exclude lines that match the *expression*.
include	(Optional) Specifies that the output display include lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display the current configured aging time for all VLANs. The fields shown in the display are self-explanatory.

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

```
Router# show mac-address-table aging-time

    Mac address aging time 300
```

Catalyst Switches

```
Router# show mac-address-table aging-time

Vlan    Aging Time
----    ----------
100     300
200     1000
```

The following example shows how to display the current configured aging time for a specific VLAN. The fields shown in the display are self-explanatory.

```
Router# show mac-address-table aging-time vlan 100

Vlan    Aging Time
----    ----------
 100    300
```

Related Commands

Command	Description
show mac-address-table address	Displays MAC address table information for a specific MAC address.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table detail	Displays detailed MAC address table information.
show mac-address-table dynamic	Displays dynamic MAC address table entries only.
show mac-address-table interface	Displays the MAC address table information for a specific interface.
show mac-address-table multicast	Displays multicast MAC address table information.
show mac-address-table protocol	Displays MAC address table information based on protocol.
show mac-address-table static	Displays static MAC address table entries only.
show mac-address-table vlan	Displays the MAC address table information for a specific VLAN.

show mac-address-table dynamic

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

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

show mac-address-table dynamic [**address** *mac-address* | **interface** *type slot/port* | **vlan** *vlan*]

Catalyst Switches

show mac-address-table dynamic [**address** *mac-address* | **detail** | **interface** *type number* | **protocol** *protocol* | | **module** *number* | **vlan** *vlan*] [[**begin** |**exclude** | **include**] *expression*]

Catalyst 6500 Series Switches

show mac-address-table dynamic [{**address** *mac-addr*} | {**interface** *interface interface-number* [**all** | **module** *number*]} | {**module** *num*} | {**vlan** *vlan-id* [**all** | **module** *number*]}]

Syntax Description

address *mac-address*	(Optional) Specifies a 48-bit MAC address; valid format is H.H.H.
detail	(Optional) Specifies a detailed display of MAC address table information.
interface *type number*	(Optional) Specifies an interface to match; valid type values are FastEthernet and GigabitEthernet, valid number values are from 1 to 9.
interface *type*	(Optional) Specifies an interface to match; valid type values are FastEthernet and GigabitEthernet.
slot	(Optional) Adds dynamic addresses to module in slot 1 or 2.
port	(Optional) Port interface number ranges 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
protocol *protocol*	(Optional) Specifies a protocol. See the "Usage Guidelines" section for keyword definitions.
module *number*	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.
vlan *vlan*	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 1005.
begin	(Optional) Specifies that the output display begin with the line that matches the expression.
exclude	(Optional) Specifies that the output display exclude lines that match the expression.
include	(Optional) Specifies that the output display include lines that match the specified expression.

expression	Expression in the output to use as a reference point.
all	(Optional) Specifies that the output display all dynamic MAC-address table entries.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XE	This command was introduced on Catalyst 6000 series switches.
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.
12.2(14)SX	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(33)SXH	This command was changed to support the **all** keyword on the Catalyst 6500 series switch.

Usage Guidelines

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

The **show mac-address-table dynamic** command output for an EtherChannel interface changes the port-number designation (for example, 5/7) to a port-group number.

Catalyst Switches

The keyword definitions for the protocol argument are:

- **ip**—Specifies IP protocol
- **ipx**—Specifies Internetwork Packet Exchange (IPX) protocols
- **assigned**—Specifies assigned protocol entries
- **other**—Specifies other protocol entries

The **show mac-address-table dynamic** command output for an EtherChannel interface changes the port-number designation (for example, 5/7) to a port-group number.

Catalyst 6500 Series Switches

The *mac-address* is a 48-bit MAC address and the valid format is H.H.H.

The optional **module** *num* keyword and argument are supported only on DFC modules. The **module** *num* keyword and argument designate the module number.

Examples

The following examples show how to display all dynamic MAC address entries. The fields shown in the various displays are self-explanatory.

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

```
Router# show mac-address-table dynamic

Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
000a.000a.000a          Dynamic       1     FastEthernet4/0
002a.2021.4567          Dynamic       2     FastEthernet4/0
```

Catalyst Switches

```
Router# show mac-address-table dynamic

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0010.0d40.37ff  dynamic        ip  --  5/8
   1  0060.704c.73ff  dynamic        ip  --  5/9
4095  0000.0000.0000  dynamic        ip  --  15/1
   1  0060.704c.73fb  dynamic     other  --  5/9
   1  0080.1c93.8040  dynamic        ip  --  5/9
4092  0050.f0ac.3058  dynamic        ip  --  15/1
   1  00e0.4fac.b3ff  dynamic     other  --  5/9
```

The following example shows how to display dynamic MAC address entries with a specific protocol type (in this case, assigned).

```
Router# show mac-address-table dynamic protocol assigned

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
4092  0000.0000.0000  dynamic  assigned  --  Router
4092  0050.f0ac.3059  dynamic  assigned  --  Router
   1  0010.7b3b.0978  dynamic  assigned  --  Fa5/9

Router#
```

The following example shows the detailed output for the previous example.

```
Router# show mac-address-table dynamic protocol assigned detail

MAC Table shown in details
=======================================
 Type   Always Learn Trap Modified Notify Capture Protocol Flood
-------+------------+----+--------+------+-------+--------+-----+
     QoS bit      L3 Spare   Mac Address  Age Byte Pvlan Xtag SWbits Index
-----------------+--------+--------------+--------+-----+----+------+-----
DYNAMIC     NO        NO     YES     NO     NO    assigned   NO
   Bit Not On        0     0000.0000.0000  255      4092   0     0     0x3

DYNAMIC     NO        NO     YES     NO     NO    assigned   NO
   Bit Not On        0     0050.f0ac.3059  254      4092   0     0     0x3

DYNAMIC     NO        NO     YES     NO     NO    assigned   NO
   Bit Not On        0     0010.7b3b.0978  254      1      0     0     0x108

Router#
```

Catalyst 6500 Series Switches

This example shows how to display all the dynamic MAC-address entries for a specific VLAN.

```
Router# show mac-address-table dynamic vlan 200 all

Legend: * - primary entry
        age - seconds since last seen
        n/a - not aevailable
vlan     mac address      type   learn    age               ports
------+----------------+--------+-----+----------+--------------------------
 200  0010.0d40.37ff   dynamic    NO      23        Gi5/8
Router#
```

This example shows how to display all the dynamic MAC-address entries.

```
Router# show mac-address-table dynamic

Legend: * - primary entry
age - seconds since last seen
n/a - not applicable
vlan     mac address      type   learn    age               ports
------+----------------+--------+-----+----------+--------------------------
* 10   0010.0000.0000   dynamic  Yes   n/a        Gi4/1
* 3    0010.0000.0000   dynamic  Yes   0          Gi4/2
* 1    0002.fcbc.ac64   dynamic  Yes   265        Gi8/1
* 1    0009.12e9.adc0   static   No    -          Router
Router#
```

Related Commands

Command	Description
show mac-address-table address	Displays MAC address table information for a specific MAC address.
show mac-address-table aging-time	Displays the MAC address aging time.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table detail	Displays detailed MAC address table information.
show mac-address-table interface	Displays the MAC address table information for a specific interface.
show mac-address-table multicast	Displays multicast MAC address table information.
show mac-address-table protocol	Displays MAC address table information based on protocol.
show mac-address-table static	Displays static MAC address table entries only.
show mac-address-table vlan	Displays the MAC address table information for a specific VLAN.

show mac-address-table learning

To display the MAC-address learning state, use the **show mac-address-table learning** command in user EXEC mode.

show mac-address-table learning [**vlan** *vlan-id* | **interface** *interface slot/port*] [**module** *num*]

Syntax Description

vlan *vlan-id*	(Optional) Displays information about the MAC-address learning state for the specified switch port VLAN; valid values are from 1 to 4094.
interface *interface slot/port*	(Optional) Displays information about the MAC-address learning state for the specified routed interface type, the slot number, and the port number.
module *num*	(Optional) Displays information about the MAC-address learning state for the specified module number.

Defaults

This command has no default settings.

Command Modes

User EXEC (>)

Command History

Release	Modification
12.2(18)SXE	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

The **module** *num* keyword and argument can be used to specify supervisor engines or Distributed Forwarding Cards (DFCs) only.

The **interface** *interface slot/port* keyword and arguments can be used on routed interfaces only. The **interface** *interface slot/port* keyword and arguments cannot be used to configure learning on switch-port interfaces.

If you specify the **vlan** *vlan-id*, the state of the MAC-address learning of the specified VLAN, including router interfaces, on all modules, is displayed.

If you specify the **vlan** *vlan-id* and the **module** *num*, the state of the MAC-address learning of a specified VLAN on a specified module is displayed.

If you specify the **interface** *interface slot/port* keyword and arguments, the state of the MAC-address learning of the specified interface on all modules is displayed.

If you specify the **interface** *interface slot/port* keyword and arguments, the state of the MAC-address learning of the specified interface on the specified module is displayed.

If you enter the **show mac-address-table learning** command with no arguments or keywords, the status of MAC learning on all the existing VLANs on all the supervisor engines or DFCs configured on a Catalyst 6500 series switch is displayed.

Examples

This example shows how to display the MAC-address learning status on all the existing VLANs on all the supervisor engines or DFCs configured on a Catalyst 6500 series switch:

```
Router# show mac-address-table learning

VLAN/Interface          Mod1   Mod4   Mod7
--------------------    ---------------------
1                       yes    yes    yes
100                     yes    yes    yes
150                     yes    yes    yes
200                     yes    yes    yes
250                     yes    yes    yes
1006                     no     no     no
1007                     no     no     no
1008                     no     no     no
1009                     no     no     no
1010                     no     no     no
1011                     no     no     no
1012                     no     no     no
1013                     no     no     no
1014                     no     no     no
GigabitEthernet6/1       no     no     no
GigabitEthernet6/2       no     no     no
GigabitEthernet6/4       no     no     no
FastEthernet3/4          no     no     no
FastEthernet3/5          no     no     no
GigabitEthernet4/1       no     no     no
GigabitEthernet4/2       no     no     no
GigabitEthernet7/1       no     no     no
GigabitEthernet7/2       no     no     no

Router#
```

Table 21 describes the fields that are shown in the example.

Table 21 show mac-address-table learning Field Descriptions

Field	Description
VLAN/Interface[1]	VLAN ID or interface type, module, and port number.
Mod#	Module number of a supervisor engine or DFC.
yes	MAC-address learning is enabled.
no	MAC-address learning is disabled.

1. The interfaces displayed are routed interfaces that have internal VLANs assigned to them.

This example shows how to display the status of MAC-address learning on all the existing VLANs on a single supervisor engine or a DFC:

```
Router# show mac-address-table learning module 4

VLAN/Interface          Mod4
--------------------    -----
1                       yes
100                     yes
150                     yes
200                     yes
250                     yes
1006                     no
1007                     no
1008                     no
```

```
1009                    no
1010                    no
1011                    no
1012                    no
1013                    no
1014                    no
GigabitEthernet6/1      no
GigabitEthernet6/2      no
GigabitEthernet6/4      no
FastEthernet3/4         no
FastEthernet3/5         no
GigabitEthernet4/1      no
GigabitEthernet4/2      no
GigabitEthernet7/1      no
GigabitEthernet7/2      no

Router#
```

This example shows how to display the status of MAC-address learning for a specific VLAN on all the supervisor engines and DFCs:

```
Router# show mac-address-table learning vlan 100

VLAN    Mod1   Mod4   Mod7
----    ---------------------
100      no     no     yes
Router
```

This example shows how to display the status of MAC-address learning for a specific VLAN on a specific supervisor engine or DFC:

```
Router# show mac-address-table learning vlan 100 module 7

VLAN    Mod7
----    -----
100     yes
Router
```

This example shows how to display the status of MAC-address learning for a specific supervisor engine or DFC:

```
Router# show mac-address-table learning interface FastEthernet 3/4

Interface       Mod1   Mod4   Mod7
---------       ---------------------
Fa3/4            no     yes    no
Router
```

This example shows how to display the status of MAC-address learning for a specific interface on a specific specific supervisor engine or DFC:

```
Router# show mac-address-table learning interface FastEthernet 3/4 module 1

Interface       Mod1
---------       -----
Fa3/4            no
Router
```

Related Commands

Command	Description
mac-address-table learning	Enables MAC-address learning.

show mac-address-table static

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

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

show mac-address-table static [**address** *mac-address* | **interface** *type slot/port* | **vlan** *vlan*]

Catalyst Switches

show mac-address-table static [**address** *mac-address* | **detail** | **interface** *type number* | **protocol** *protocol* | **vlan** *vlan-id*] [[**begin** | **exclude** | **include**] *expression*]

Syntax Description

address *mac-address*	(Optional) Specifies a 48-bit MAC address to match; valid format is H.H.H.
detail	(Optional) Specifies a detailed display of MAC address table information.
interface *type number*	(Optional) Specifies an interface to match; valid type values are Ethernet, FastEthernet, and Gigabit Ethernet and valid number values are from 1 to 9.
interface *type*	(Optional) Specifies an interface to match; valid type values are FastEthernet and Gigabit Ethernet.
slot	(Optional) Adds dynamic addresses to module in slot 1 or 2.
port	(Optional) Port interface number ranges 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 Gigabit Ethernet
protocol *protocol*	(Optional) Specifies a protocol. See the "Usage Guidelines" section for keyword definitions.
vlan *vlan*	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 1005.
begin	(Optional) Specifies that the output display begin with the line that matches the expression.
exclude	(Optional) Specifies that the output display exclude lines that match the expression.
include	(Optional) Specifies that the output display include lines that match the expression.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (#)

Command History

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

Catalyst Switches

The keyword definitions for the protocol argument are:

- **ip**—Specifies IP protocol
- **ipx**—Specifies Internetwork Packet Exchange (IPX) protocols
- **assigned**—Specifies assigned protocol entries
- **other**—Specifies other protocol entries

Examples

The following examples show how to display all static MAC address entries. The fields shown in the various displays are self-explanatory.

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

```
Router# show mac-address-table static

Static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
2323.3214.5432          Static        4     FastEthernet4/1
2323.3214.5431          Static        5     FastEthernet4/1
2323.3214.5432          Static        6     FastEthernet4/1
2323.3214.5434          Static        7     FastEthernet4/1
2323.3214.5435          Static        8     FastEthernet4/1
```

Catalyst Switches

```
Router# show mac-address-table static

*Oct 22 12:15:35: %SYS-5-CONFIG_I: Configured from console by console
vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0050.3e8d.6400  static   assigned  --  Router
 100  0050.3e8d.6400  static   assigned  --  Router
4092  0050.f0ac.3058  static      other  --  Router
 917  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
   5  0050.3e8d.6400  static   assigned  --  Router
 303  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 850  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
1002  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 802  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
```

```
   2  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 304  0100.5e00.0001  static         ip  --  Fa5/9,Switch
.
.
.
```

The following example shows how to display static MAC address entries with a specific protocol type (in this case, assigned).

```
Router# show mac-address-table static protocol assigned

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0050.3e8d.6400  static   assigned  --  Router
 100  0050.3e8d.6400  static   assigned  --  Router
   5  0050.3e8d.6400  static   assigned  --  Router
```

The following example shows the detailed output for the previous example.

```
Router# show mac-address-table static protocol assigned detail

       MAC Table shown in details
=======================================
 Type   Always Learn Trap Modified Notify Capture Protocol Flood
-------+------------+----+--------+------+-------+--------+-----+
     QoS bit      L3 Spare   Mac Address  Age Byte Pvlan Xtag SWbits Index
-----------------+--------+--------------+--------+-----+----+------+-----
STATIC      NO        NO     NO      NO     NO    assigned   NO
   Bit Not On        0     0050.3e8d.6400  254      200    1     0     0x3

STATIC      NO        NO     NO      NO     NO    assigned   NO
   Bit Not On        0     0050.3e8d.6400  254      100    1     0     0x3

STATIC      NO        NO     NO      NO     NO    assigned   NO
   Bit Not On        0     0050.3e8d.6400  254      5      1     0     0x3

S   Bit Not On        0     0050.f0ac.3058  254      4092   1     0     0x3
.
.
.
```

Cisco 7600 Series Routers

This example shows how to display all the static MAC address entries; this Catalyst 6500 series switch is configured with a Supervisor Engine 720.

```
Router# show mac-address-table static

Codes: * - primary entry

  vlan   mac address     type    learn qos            ports
------+---------------+--------+-----+---+--------------------------
*  ---  0001.6441.60ca    static  No    --  Router
```

Related Commands

Command	Description
show mac-address-table address	Displays MAC address table information for a specific MAC address.
show mac-address-table aging-time	Displays the MAC address aging time.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table detail	Displays detailed MAC address table information.
show mac-address-table dynamic	Displays dynamic MAC address table entries only.
show mac-address-table interface	Displays the MAC address table information for a specific interface.
show mac-address-table multicast	Displays multicast MAC address table information.
show mac-address-table protocol	Displays MAC address table information based on protocol.
show mac-address-table vlan	Displays the MAC address table information for a specific VLAN.

show mls df-table

To display information about the multilayer switching (MLS) Don't Fragment (DF) table, use the **show mls df-table** command in privileged EXEC mode.

show mls df-table *start-vlan end-vlan*

Syntax Description

start-vlan	Start of a range of VLAN IDs; valid values are from 1 to 4094.
end-vlan	End of a range of VLAN IDs; valid values are from 1 to 4094.

Command Modes

Privileged EXEC (#)

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.

You must identify the active Supervisor Engine by using the **show module** command; and start a command-line interface sesssion with the active Supervisor Engine by using the **attach** command in privileged EXEC mode, before you can use the **show mls df-table** command.

In the output display, the following applies:

- 1 indicates that DF is enabled.
- 0 indicates that DF is disabled.

Examples

This example shows how to display the DF-table contents on the Supervisor Engine for a range of VLANs. The fields shown in the display are self-explanatory.

```
Router# remote login switch

Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session


Router-sp#

Router-sp# show mls df-table 201 212

TYCHO FIB DF Table

vlan   df_index
       3 2 1 0
-----+----------
 201   0 0 0 0
 202   0 0 0 0
```

```
 203    0 0 0 0
 204    0 0 0 0
 205    0 0 0 0
 206    0 0 0 0
 207    0 0 0 0
 208    0 0 0 0
 209    0 0 0 0
 210    0 0 0 0
 211    0 0 0 0
 212    0 0 0 0
Router-sp#
```

Related Commands

Command	Description
show mls asic	Displays the ASIC version.
show mls ip	Displays the MLS IP information.
show mls ipx	Displays the MLS IPX information.
show mls qos	Displays MLS QoS information.
show mls statistics	Displays the MLS statistics for the IP.

show mls masks

To display the details of the access control parameters (ACPs) that are used for multilayer switching (MLS) quality of service (QoS) and security access control lists (ACLs), use the **show mls masks** command in privileged EXEC mode.

show mls masks [**qos** | **security**]

Syntax Description

qos	(Optional) Displays details of ACPs used for QoS ACLs.
security	(Optional) Displays details of ACPs used for security ACLs.

Note ACPs are called masks in the command-line interface (CLI) commands and output.

Command Modes

Privileged EXEC (#)

Command History

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

Use the **show mls mask** command without keywords to display all ACPs configured on the switch.

Use this command with the **qos** keyword to display the ACPs used for QoS ACLs.

Use this command with the **security** keyword to display the ACPs used for security ACLs.

Note You can configure up to four ACPs (QoS and security) on a switch.

Examples

The following is sample output from the **show mls masks** command. In this example, Mask 1 is a QoS ACP consisting of an IP source address (with wildcard bits 0.0.0.255), an IP destination address, and Layer 4 destination port fields. This ACP is used by the QoS policy maps pmap1 and pmap2.

The fields shown in the display are self-explanatory.

```
Router# show mls masks

Mask1
        Type : qos
        Fields : ip-sa(0.0.0.255), ip-da(host), dest-port
        Policymap: pmap1
            Interfaces: Fa0/9, Gi0/1
        Policymap: pmap2
            Interfaces: Fa0/1, Fa0/5, Fa0/13
```

Related Commands

Command	Description
ip access-group	Applies an IP ACL to an interface.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

show mls rp

To display multilayer switching (MLS) details, including specifics for the Multilayer Switching Protocol (MLSP), use the **show mls rp** command in user EXEC mode or privileged EXEC mode.

show mls rp [*interface*]

Syntax Description

interface	(Optional) Displays information for one interface. Without this argument, detailed views of all interfaces are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(3)WA4(4)	This command was introduced.
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.

Examples

The following is sample output from the **show mls rp** command. The fields shown in the display are self-explanatory.

```
Router# show mls rp

multilayer switching is globally enabled
mls id is 00e0.fefc.6000
mls ip address 10.20.26.64
mls flow mask is ip-flow
vlan domain name: WBU
   current flow mask: ip-flow
   current sequence number: 80709115
   current/maximum retry count: 0/10
   current domain state: no-change
   current/next global purge: false/false
   current/next purge count: 0/0
   domain uptime: 13:03:19
   keepalive timer expires in 9 seconds
   retry timer not running
   change timer not running
   fcp subblock count = 7

   1 management interface(s) currently defined:
      vlan 1 on Vlan1

   7 mac-vlan(s) configured for multi-layer switching:

      mac 00e0.fefc.6000
         vlan id(s)
         1    10   91   92   93   95   100
```

```
   router currently aware of following 1 switch(es):
      switch id 0010.1192.b5ff
```

The following is sample output from the **show mls rp** command for a specific interface:

```
Router# show mls rp int vlan 10

mls active on Vlan10, domain WBU
```

Related Commands

Command	Description
mls rp ip	Enables MLSP.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp nde-address	Specifies a NetFlow Data Export address.
mls rp vlan-id	Assigns a VLAN ID.
mls rp vtp-domain	Selects the router interface to be Layer 3 switched and then adds that interface to a VTP domain.
show mls rp vtp-domain	Displays MLS interfaces for a specific VTP domain.

show mls rp interface

To display Internetwork Packet Exchange (IPX) multilayer switching (MLS) details for the route processor (RP), including specific information about the Multilayer Switching Protocol (MLSP), use the **show mls rp interface** command in user EXEC mode or privileged EXEC mode.

show mls rp interface *type number*

Syntax Description

type	Interface type.
number	Interface number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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.

Examples

The following displays sample output from the **show mls rp interface** command. The interface type is VLAN, and its number is 10. The fields shown in the display are self-explanatory.

```
Router# show mls rp interface vlan 10

    IPX MLS active on Vlan 10, domain WBU
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the route processor.

show mls rp ip multicast

To display hardware-switched multicast flow information about IP multicast multilayer switching (MLS), use the **show mls rp ip multicast** command in user EXEC mode or privileged EXEC mode.

show mls rp ip multicast [**locate**] [*group* [*source*] [*vlan-id*]] [**statistics**] [**summary**]

Syntax Description

locate	(Optional) Displays flow information associated with the switch. This keyword applies only to a single router and multiple switches.
group	(Optional) Address of the IP multicast group about which to display information.
source	(Optional) IP multicast source sending to the specified multicast group about which to display information.
vlan-id	(Optional) Source VLAN about which to display information.
statistics	(Optional) Displays MLS statistics.
summary	(Optional) Displays MLS summary.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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.

Examples

The following is sample output of the **show mls rp ip multicast** command using the **locate** keyword:

```
Router# show mls rp ip multicast locate

Source           Group            Vlan  SwitchIP         SwitchMAC
------           -----            ----  --------         ---------
192.168.10.6     239.255.158.197  10    192.168.10.199   0010.a60b.b4ff
```

The following is sample output of the **show mls rp ip multicast** command for a specific IP multicast group:

```
Router# show mls rp ip multicast 224.1.1.1

Multicast hardware switched flows:
(10.1.13.1, 224.1.1.1) Incoming interface: Vlan13, Packets switched: 61590
Hardware switched outgoing interfaces: Vlan20 Vlan9
MFD installed: Vlan13

(10.1.9.3, 224.1.1.1) Incoming interface: Vlan9, Packets switched: 0
Hardware switched outgoing interfaces: Vlan20
MFD installed: Vlan9
```

```
(10.1.12.1, 224.1.1.1) Incoming interface: Vlan12, Packets switched: 62010
Hardware switched outgoing interfaces: Vlan20 Vlan9
MFD installed: Vlan12

(10.1.12.3, 224.1.1.1) Incoming interface: Vlan12, Packets switched: 61980
Hardware switched outgoing interfaces: Vlan20 Vlan9
MFD installed: Vlan12

(10.1.11.1, 224.1.1.1) Incoming interface: Vlan11, Packets switched: 62430
Hardware switched outgoing interfaces: Vlan20 Vlan9
MFD installed: Vlan11

(10.1.11.3, 224.1.1.1) Incoming interface: Vlan11, Packets switched: 62430
Hardware switched outgoing interfaces: Vlan20 Vlan9
MFD installed: Vlan11

Total shortcut installed: 6
```

The following is sample output of the **show mls rp ip multicast** command using the **statistics** keyword:

```
Router# show mls rp ip multicast statistics

MLS Multicast Operation Status:
MLS Multicast configuration and state:
    Router Mac: 0010.298f.0009
    Switch Mac: 0010.0d70.a3ff      Switch IP: 10.2.10.195
    MLS Multicast Operating state: ACTIVE
    Active management vlan: Vlan1, 192.1.4.1
    User configured management vlan: None, 0.0.0.0
    Include-List: IP1 = 192.168.28.2, IP2 = 10.0.0.0
    Router IP used in MLS Multicast messages: 192.168.28.2

MLS Multicast statistics:
    Keepalive sent: 90
    Keepalive ACK received: 90
    Open request sent: 3
    Open request ACK received: 3
    Delete notifications received: 3
    Flow statistics messages received: 181
    Flow message sent: 14
    Flow message Ack received: 14
    Flow message Nack received: 0

    Flow install Ack: 2
    Flow install Nack: 0
    Flow update Ack: 7
    Flow update Nack: 0
    Flow delete Ack: 0
    Complete flow install Ack: 3
    Complete flow install Nack: 0
    Complete flow delete Ack: 1
    Input vlan delete Ack: 0
    Output vlan delete Ack: 0
    Global delete sent: 1

    L2 entry not found error: 0
    LTL entry not found error: 0
    MET entry not found error: 0
    L3 entry not found error: 0
    L3 entry exists error : 0
    Hash collision error : 0
```

```
    Sequence number error : 0
    None-supported error : 0
    Generic error : 0
```

The following is sample output of the **show mls rp ip multicast** command using the **summary** keyword:

```
Router# show mls rp ip multicast summary

Switch IP:10.0.0.0  Switch MAC:0000.0000.0000
Number of complete flows: 0
Total hardware-switched flows: 0

Switch IP:10.2.10.199  Switch MAC:0010.a60b.b4ff
Number of complete flows: 1
Total hardware-switched flows: 1
```

Related Commands

Command	Description
mls rp ip multicast	Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.

show mls rp ipx

To display details for all Internetwork Packet Exchange (IPX) multilayer switching (MLS) interfaces on the IPX MLS router, use the **show mls rp ipx** command in privileged EXEC mode.

show mls rp ipx

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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

This command gives you details about the following:

- MLS status (enabled or disabled) for switch interfaces and subinterfaces
- Flow mask required when creating Layer 3 switching entries for the router
- Current settings for the keepalive timer, retry timer, and retry count
- MLS identifier used in Multilayer Switching Protocol (MLSP) messages
- List of all interfaces in all Virtual Trunking Protocol (VTP) domains enabled for MLS

Examples

The following example shows sample output from the **show mls rp ipx** command for all IPX MLS interfaces on an MLS route processor (RP). The fields shown in the display are self-explanatory.

```
Router# show mls rp ipx

    ipx multilayer switching is globally enabled
    ipx mls inbound acl override is globally disabled
    mls id is 0050.73ff.b580
    mls ip address 5.5.5.155
    IPX MLS flow mask is source-destination
    number of domains configured for mls 1

    vlan domain name:Engineering
           current ipx flow mask:source-destination
           ipx current/next global purge:false/false
           ipx current/next purge count:0/0
           current sequence number:4086390283
           current/maximum retry count:0/10
           current domain state:no-change
           domain uptime:03:13:09
           keepalive timer expires in 3 seconds
```

```
    retry timer not running
    change timer not running

1 management interface(s) currently defined:
       vlan 21 on Vlan21

2 mac-vlan(s) enabled for ipx multi-layer switching:

       mac 0010.0738.2917
          vlan id(s)
          22

       mac 0050.73ff.b5b8
          vlan id(s)
          21

router currently aware of following 1 switch(es):
       switch id 00e0.fe4a.aeff
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

show mls rp vtp-domain

To display Internetwork Packet Exchange (IPX) multilayer switching (MLS) interfaces for a specific Virtual Trunking Protocol (VTP) domain on a Route Processor (RP), use the **show mls rp vtp-domain** command in privileged EXEC mode.

show mls rp vtp-domain *domain-name*

Syntax Description

domain-name	The name of the VTP domain whose MLS interfaces will be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(3)WA4(4)	This command was introduced.
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.

Examples

This example shows details about IPX MLS interfaces in a VTP domain named WBU. The fields shown in the display are self-explanatory.

```
Router# show mls rp vtp-domain WBU

    vlan domain name: WBU
    current ipx flow mask: destination
           ipx current/next global purge: false/false
           ipx current/next purge count: 0/0
           current ipx flow mask: destination
           ipx current/next global purge: false/false
           ipx current/next purge count: 0/0
           current sequence number: 590678296
           current/maximum retry count: 0/10
           current domain state: no-change
           domain uptime: 1d14h
           keepalive timer expires in 3 seconds
           retry timer not running
           change timer not running
           fcp subblock count = 20

       1 management interface(s) currently defined:
              vlan 2 on Vlan2

       20 mac-vlan(s) configured for multi-layer switching

       17 mac-vlan(s) enabled for ipx multi-layer switching:

              mac 0010.0738.2917
                 vlan id(s)
         2    3    4    5    6    7    8    9    10   12   13
         14   15   88   99
```

```
       mac 0090.6dfc.5800
          vlan id(s)
          20   21

18 mac-vlan(s) enabled for ipx multi-layer switching:

       mac 0010.0738.2917
          vlan id(s)
          2    3    4    5    6    7    8    9    10   11   12
          13   14   15   66   77   88   99

router currently aware of following 1 switch(es):
       switch id 0010.141f.6fff
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

show mmls igmp explicit-tracking

To display information about the host-tracking database, use the **show mmls igmp explicit-tracking** command in privileged EXEC mode.

show mmls igmp explicit-tracking [*vlan-id*]

Syntax Description

vlan-id	(Optional) VLAN ID; valid values are 1 to 4094.

Command Modes

Privileged EXEC (#)

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 display information about the host-tracking database for a specific VLAN. The fields shown in the display are self-explanatory.

```
Switch-sp# show mmls igmp explicit-tracking 27

Source/Group                    Interface    Reporter        Filter_mode
------------------------------------------------------------------------
10.1.1.1/224.1.1.1              Vl27:3/25    10.27.2.3       INCLUDE
10.2.2.2/224.1.1.1              Vl27:3/25    10.27.2.3       INCLUDE
Router#
```

show mmls msc

To display information about Multicast Multilayer Switching (MMLS), use the **show mmls msc** command in privileged EXEC mode.

show mmls msc [**cache** | **entry** | **icroif-cache** | **rpdf-cache** | **statistics** | **vpn**]

Syntax Description

cache	(Optional) Displays information about the multicast shortcuts for the process cache.
entry	(Optional) Displays information about the dump-hardware entries in Layer 3.
icroif-cache	(Optional) Displays information about the dump-ICROIF cache.
rpdf-cache	(Optional) Displays information about the dump-bidirectional (Bidir) RPDF cache.
statistics	(Optional) Displays statistics on the multicast-shortcuts process.
vpn	(Optional) Displays information about Virtual Private Networks (VPNs).

Command Default

MMLS information is not displayed.

Command Modes

Privileged EXEC (#)

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 display information about MMLS. The fields are self-explanatory.

```
Router# remote login switch
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session


Router#

Router# show mmls msc

     General Info
     ------------------------------------------------------+-------+
     Number shortcuts in software database                 1890
     Number of MFD in software database                    1890
     Router MAC                                            0001.64f8.1b00
```

```
     Internal Vlan                                    4093
     Aggregation Vlan                                 0
     Aggregation Indexes                              0
     Current Size of inputQ                           0
     Maximum Size of inputQ                           2
     flow statistics timeout [sec]                    25
     non-rpf MFDs purge timeout [sec]                 20
     non-rpf MFDs aging timeout [sec]                 2.0
Router#
```

This example shows how to display information about the MMLS shortcut-process cache:

```
Router# show mmls msc cache

     -------------macg cache buckets for vpn 0-----------------
     Bucket 90 #g: 1
     Group mac address: 0100.5e01.0105
       $$$ (S,G,C): (10.0.0.4, 224.1.1.5, 100)      mfd_flag: 1  type: Sparse
       $$$ (S,G,C): (0.0.0.0, 224.1.1.5, 1)      mfd_flag: 1  type: Sparse
       ### vlan:  100   sc_count:     0 rpf_count:     1
       ### vlan:    1   sc_count:     0 rpf_count:     1
     Bucket 91 #g: 1
     Group mac address: 0100.5e01.0104
       $$$ (S,G,C): (10.0.0.4, 224.1.1.4, 100)      mfd_flag: 1  type: Sparse
       $$$ (S,G,C): (0.0.0.0, 224.1.1.4, 1)      mfd_flag: 1  type: Sparse
       ### vlan:  100   sc_count:     0 rpf_count:     1
       ### vlan:    1   sc_count:     0 rpf_count:     1
     Bucket 92 #g: 1
     Group mac address: 0100.5e01.0103
       $$$ (S,G,C): (10.0.0.4, 224.1.1.3, 100)      mfd_flag: 1  type: Sparse
       $$$ (S,G,C): (0.0.0.0, 224.1.1.3, 1)      mfd_flag: 1  type: Sparse
       ### vlan:  100   sc_count:     0 rpf_count:     1
       ### vlan:    1   sc_count:     0 rpf_count:     1
     Bucket 93 #g: 1
     Group mac address: 0100.5e01.0102
       $$$ (S,G,C): (10.0.0.4, 224.1.1.2, 100)      mfd_flag: 1  type: Sparse
       $$$ (S,G,C): (0.0.0.0, 224.1.1.2, 1)      mfd_flag: 1  type: Sparse
       ### vlan:  100   sc_count:     0 rpf_count:     1
       ### vlan:    1   sc_count:     0 rpf_count:     1
     Bucket 94 #g: 1
     Group mac address: 0100.5e01.0101
       $$$ (S,G,C): (10.0.0.4, 224.1.1.1, 100)      mfd_flag: 1  type: Sparse
       $$$ (S,G,C): (0.0.0.0, 224.1.1.1, 1)      mfd_flag: 1  type: Sparse
       ### vlan:  100   sc_count:     0 rpf_count:     1
       ### vlan:    1   sc_count:     0 rpf_count:     1
Router#
```

This example shows how to display dump ICROIF-cache information:

```
Router# show mmls msc icroif-cache

     msc_local_icroif_index:  0x493
     msc_global_icroif_index: 0x494

     ICROIF CACHE:
     -------------
     Module mask: 0x8       Icroif_index: 0x495
Router#
```

This example shows how to display a dump list of DF interfaces for the PIM-RPs:

```
Router# show mmls msc rpdf-cache

--------------- RP-CACHE [VPN-0] --------------
```

```
Bucket# :0

        RP-addr: 10.1.0.1, Rpf: 0 Vpn: 0
        DF-index: 0
        DF-list:  201  202  203  204  205  206  207  208  209  210
                  211  212
        Group-list:
                (224.1.0.0/24, H)
        G/m-count: 1, G/32-count: 1

Bucket# :2

        RP-addr: 10.3.0.1, Rpf: 0 Vpn: 0
        DF-index: 2
        DF-list:  201  202  203  204  205  206  207  208  209  210
                  211  212
        Group-list:
                (224.1.2.0/24, H)
        G/m-count: 1, G/32-count: 0

Bucket# :3

        RP-addr: 10.2.0.1, Rpf: 0 Vpn: 0
        DF-index: 1
        DF-list:  201  202  203  204  205  206  207  208  209  210
                  211  212
        Group-list:
                (224.1.1.0/24, H)
        G/m-count: 1, G/32-count: 1

Bucket# :5

        RP-addr: 10.4.0.1, Rpf: 0 Vpn: 0
        DF-index: 3
        DF-list:  201  202  203  204  205  206  207  208  209  210
                  211  212
        Group-list:
                (224.1.3.0/24, H)
        G/m-count: 1, G/32-count: 0
Router#
```

This example shows how to display the statistics for the multicast-shortcut process:

```
Router# show mmls msc statistics

     Communication Statistics
     ------------------------------------------------+------+
     Number MSM PDU Received                           1
     Number MSM PDU Sent                               1
     Unsolicited Feature Notification Sent             1
     Feature Notification Received                     2
     Feature Notification Sent                         2
     Stop retry  Sent                                  0
     Stop download Sent                                0

     Error Statistics
     ------------------------------------------------+------+
     L2 entry not found                                0
     LTL full error                                    0
     MET full error                                    0

     Debug Statistics
     ------------------------------------------------+------+
```

```
HW Met failure                                    0
HW Dist failure                                   0
HW L3 Install failure                             0
HW L3 Update failure                              0

TLV Statistics
-------------------------------------------------+------+
INSTALL TLV Received                              0
SELECTIVE DELETE TLV Received                     0
GROUP DELETE TLV Received                         0
UPDATE TLV Received                               0
INPUT VLAN DELETE TLV Received                    0
OUTPUT VLAN DELETE TLV Received                   0
GLOBAL DELETE TLV Received                        0
MFD INSTALL TLV Received                          0
MFD DELETE TLV Received                           0
MFD GLOBAL DELETE Received                        0
NRPF MFD INSTALL TLV Received                     0
NRPF MFD DELETE TLV Received                      0
SUBNET INSTALL TLV Received                       15
SUBNET DELETE TLV Received                        0
MVPN INSTALL TLV Received                         0
MVPN SELECTIVE DELETE TLV Received                0
MVPN UPDATE TLV Received                          0
MVPN GROUP DELETE TLV Received                    0
MVPN MFD INSTALL TLV Received                     0
MVPN MFD DELETE TLV Received                      0
MVPN BIDIR RPDF UPDATE TLV Received               0
MVPN BIDIR RP UPDATE TLV Received                 0
MVPN BIDIR CLEAR ALL GRP TLV Received             0
MVPN BIDIR CLEAR RP GRP TLV Received              0
MVPN BIDIR CLEAR ALL DF TLV Received              0
MVPN BIDIR CLEAR RP DF TLV Received               0
MVPN BIDIR CLEAR ALL RP TLV Received              0
MVPN BIDIR NONDF INSTALL TLV Received             0

INSTALL TLV Ack Sent                              0
SELECTIVE DELETE TLV Ack Sent                     0
GROUP DELETE TLV Ack Sent                         0
UPDATE TLV Ack Sent                               0
INPUT VLAN DELETE TLV Ack Sent                    0
OUTPUT VLAN DELETE TLV Ack Sent                   0
GLOBAL DELETE TLV Ack Sent                        0
MFD INSTALL TLV Ack Sent                          0
MFD DELETE TLV Ack Sent                           0
MFD GLOBAL DELETE Ack Sent                        0
NRPF MFD INSTALL TLV Ack Sent                     0
NRPF MFD DELETE TLV Ack Sent                      0
SUBNET INSTALL TLV Ack Sent                       15
SUBNET DELETE TLV Ack Sent                        0
MVPN INSTALL TLV Ack Sent                         0
MVPN SELECTIVE DELETE TLV Ack Sent                0
MVPN UPDATE TLV Ack Sent                          0
MVPN GROUP DELETE TLV Ack Sent                    0
MVPN MFD INSTALL TLV Ack Sent                     0
MVPN MFD DELETE TLV Ack Sent                      0
MVPN BIDIR RPDF UPDATE TLV Ack Sent               0
MVPN BIDIR RP UPDATE TLV Ack Sent                 0
MVPN BIDIR CLEAR ALL GRP TLV Ack Sent             1
MVPN BIDIR CLEAR RP GRP TLV Ack Sent              0
MVPN BIDIR CLEAR ALL DF TLV Ack Sent              0
MVPN BIDIR CLEAR RP DF TLV Ack Sent               0
MVPN BIDIR CLEAR ALL RP TLV Ack Sent              0
MVPN BIDIR NONDF INSTALL TLV Ack Sent             0
```

```
     TLV Error Statistics
     ------------------------------------------------+------+
     Generic error                                    0
     L3 entry exist error                             0
     Hash collision error                             0
     L3 entry not found                               0
     MFD exist error                                  0
     MFD not found error                              0
     Invalid subnet error                             0
     Bidir-RP not found error                         0
     Bidir-DF partial fail error                      0
     Bidir-DF Table full error                        0

     TLV Debug Statistics
     ------------------------------------------------+------+
     Non RPF L3 failure                               0
     Bidir DF install                                 0
     Bidir DF failure                                 0
     Bidir NDF install                                0
     Bidir NDF failure                                0
     Bidir DF err-tlv sent                            0
     Bidir GRP err-tlv sent                           0
Router#
```

Related Commands

Command	Description
show mls asic	Displays the ASIC version.
show mls df-table	Displays information about the DF table.
show mls ip	Displays the MLS IP information.
show mls ipx	Displays the MLS IPX information.
show mls qos	Displays MLS QoS information.
show mls statistics	Displays the MLS statistics for the IP.

show mvrp interface

To display Multiple VLAN Registration Protocol (MVRP) interface states, use the **show mvrp interface** command in privileged EXEC mode.

show mvrp interface [*type slot/port*] [**statistics**]

Syntax Description

type slot/port	(Optional) The interface for which information is displayed.
statistics	(Optional) Displays MVRP statistics information for the MVRP port.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display MVRP interface details of the administrative and operational MVRP states of all or one particular IEEE 802.1q trunk port in the device.

Examples

The following example shows sample output. The fields are self-explanatory.

```
Router# show mvrp interface

Port      Status   Registrar State
Fa3/1     off      normal

Port      Join Timeout   Leave Timeout   Leaveall Timeout
Fa3/1     201 600        700             1000

Port      Vlans Declared
Fa3/1     none

Port      Vlans Registered
Fa3/1     none

Port      Vlans Registered and in Spanning Tree Forwarding State
Fa3/1     none
```

Related Commands

Command	Description
show mvrp summary	Displays the MVRP configuration at the device level.

show mvrp module

To display Multiple VLAN Registration Protocol (MVRP)-related information for a specific module, use the **show mvrp module** command in privileged EXEC mode.

show mvrp module *module-number*

Syntax Description

module-number	Indicates the module for which information is displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display MVRP module details of the administrative and operational MVRP states of all or one particular IEEE 802.1q trunk port in the device.

Examples

The following example shows sample summary output. The fields are self-explanatory.

```
Router# show mvrp module 3

Port      Status   Registrar State
Fa3/1     off      normal

Port      Join Timeout   Leave Timeout   Leaveall Timeout
Fa3/1     201          700             1000
Fa3/5    201           700             1000

Port      Vlans Declared
Fa3/1     none
Fa3/5      3,100

Port      Vlans Registered
Fa3/1     none
Fa3/5      3,100

Port      Vlans Registered and in Spanning Tree Forwarding State
Fa3/1     none
Fa3/5      3
```

Related Commands

Command	Description
show mvrp summary	Displays the MVRP configuration at the device level.

show mvrp summary

To display the Multiple VLAN Registration Protocol (MVRP) configuration at the device level, use the **show mvrp summary** command in privileged EXEC mode.

show mvrp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display MVRP configuration details.

Examples

The following example shows sample summary output for a device with MVRP configured. The fields are self-explanatory.

```
Router# show mvrp summary

MVRP global state           : enabled
MVRP VLAN creation          : disabled
VLANs created via MVRP      : 20-45, 3001-3050
Learning disabled on VLANs: none
```

Related Commands

Command	Description
show mvrp interface	Displays details of the administrative and operational MVRP states of all or one particular IEEE 802.1q trunk port in the device.

show platform software status control-processor

To display status information about the control processors, use the **show platform software status control-processor** command in privileged EXEC or diagnostic mode.

show platform software status control-processor [**brief**]

Syntax Description

brief	(Optional) Displays summary status information for the control processors.

Command Modes

Privileged EXEC (#)
Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	This command was modified. The **brief** keyword was added.

Usage Guidelines

Control processors consist of Embedded Services Processors (ESPs), Route Processors (RPs), and SPA Interface Processors (SIPs).

Use the **show platform software status control-processor** command to provide a quick view of the health of the system concerning memory and CPU usage on each processor.

The CPU usage output reflects the relative percentage of CPU usage during the latest two seconds instead of the cumulative percent usage over the entire uptime.

All control processors should show a status of Healthy. Other possible status values are Warning and Critical. Warning indicates that the router is operational but that the operating level should be reviewed. Critical implies that the router is near failure.

If you see a status of Warning or Critical, take the following actions:

- Reduce static and dynamic loads on the system by reducing the number of elements in the configuration or by limiting the capacity for dynamic services.
- Reduce the number of routes and adjacencies, limit the number of ACLs and other rules, reduce the number of VLANs, and so on.

Examples

The following example displays status information about the control processors:

```
Router# show platform software status control-processor

RP0: online, statistics updated 7 seconds ago
Load Average: healthy
  1-Min: 0.16, status: healthy, under 5.00
  5-Min: 0.16, status: healthy, under 5.00
  15-Min: 0.12, status: healthy, under 5.00
```

```
Memory (kb): healthy
  Total: 3733016
  Used: 1320804 (31%)
  Free: 2412212 (58%)
  Committed: 1889524 (45%), status: healthy, under 90%

ESP0: online, statistics updated 7 seconds ago
Load Average: healthy
  1-Min: 0.00, status: healthy, under 5.00
  5-Min: 0.00, status: healthy, under 5.00
  15-Min: 0.00, status: healthy, under 5.00
Memory (kb): healthy
  Total: 984996
  Used: 532492 (50%)
  Free: 452504 (43%)
  Committed: 1724096 (164%), status: healthy, under 300%

SIP0: online, statistics updated 10 seconds ago
Load Average: healthy
  1-Min: 0.00, status: healthy, under 5.00
  5-Min: 0.00, status: healthy, under 5.00
  15-Min: 0.00, status: healthy, under 5.00
Memory (kb): warning
  Total: 479884
  Used: 434476 (82%)
  Free: 45408 (8%)
  Committed: 202508 (38%), status: healthy, under 90%

SIP1: online, statistics updated 10 seconds ago
Load Average: healthy
  1-Min: 0.00, status: healthy, under 5.00
  5-Min: 0.00, status: healthy, under 5.00
  15-Min: 0.00, status: healthy, under 5.00
Memory (kb): warning
  Total: 479884
  Used: 430384 (82%)
  Free: 49500 (9%)
  Committed: 202512 (38%), status: healthy, under 90%
```

The following example displays summary status information about the control processors with **brief** keyword:

```
Router# show platform software status control-processor brief

Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   0.25   0.30   0.44
  RP1 Healthy   0.31   0.19   0.12
 ESP0 Healthy   0.01   0.05   0.02
 ESP1 Healthy   0.03   0.05   0.01
 SIP1 Healthy   0.15   0.07   0.01
 SIP2 Healthy   0.03   0.03   0.00

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  3722408  2514836 (60%)  1207572 (29%)   1891176 (45%)
  RP1 Healthy  3722408  2547488 (61%)  1174920 (28%)   1889976 (45%)
 ESP0 Healthy  2025468  1432088 (68%)   593380 (28%)   3136912 (149%)
 ESP1 Healthy  2025468  1377980 (65%)   647488 (30%)   3084412 (147%)
 SIP1 Healthy   480388   293084 (55%)   187304 (35%)    148532 (28%)
 SIP2 Healthy   480388   273992 (52%)   206396 (39%)     93188 (17%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
```

```
  RP0    0  30.12   1.69   0.00  67.63   0.13   0.41   0.00
  RP1    0  21.98   1.13   0.00  76.54   0.04   0.12   0.16
 ESP0    0  13.37   4.77   0.00  81.58   0.07   0.19   0.00
 ESP1    0   5.76   3.56   0.00  90.58   0.03   0.05   0.00
 SIP1    0   3.79   0.13   0.00  96.04   0.00   0.02   0.00
 SIP2    0   3.50   0.12   0.00  96.34   0.00   0.02   0.00
```

Table 22 describes the significant fields shown in the display.

Table 22 show platform software status control-processor Field Descriptions

Field	Description
processor-name: online	Name of the online control processor to which the statistics that follow apply.
statistics updated *x* seconds ago	Time (in seconds) when the statistics were last updated.
Load Average:	Summary status indicator of the overall control processor load average. This value is derived from the "5-Min" load average.
1-Min: / status:	One-minute load average on the control processor and status indicator.
5-Min: / status:	Five-minute load average on the control processor and status indicator.
15-Min: / status:	Fifteen-minute load average on the control processor and status indicator.
Memory (kb):	Summary status indicator of the overall control processor memory usage. This value signals if any of the individual memory values below are in critical or warning status.
Total:	Total memory (in kilobytes) on the control processor.
Used: *xxxxxxx* (*pp%*)	Total used memory (in kilobytes) on the control processor and the percentage of used memory on the control processor.
Free: *xxxxxxx* (*pp%*)	Total free memory (in kilobytes) on the control processor and the percentage of free memory on the control processor.
Committed: *xxxxxxx* (*pp%*) / status:	Total committed memory (in kilobytes) on the control processor, percentage of committed memory on the control processor, and status indicator.
CPU Utilization:	Percentage of time that the CPU is busy.
CPU:	Allocated processor.
User:	Non-Linux kernel processes.
System:	Linux kernel process.
Nice:	Low priority processes.
Idle:	Percentage of time that the CPU was inactive.
IRQ:	Interrupts.
SIRQ:	System interrupts.
IOwait:	Percentage of time that the CPU was waiting for I/O.

Related Commands

Command	Description
show platform software process list	Displays a list of the processes running in a given slot.

show port flowcontrol

To display per-port status information and statistics related to flow control, use the **show port flowcontrol** command in privileged EXEC mode.

show port flowcontrol [*module-number*[*/port-number*]]

Syntax Description

module-number	(Optional) Number of the module.
/port-number	(Optional) Number of the port on the module. If you do not specify a number, filters configured on all the ports on the module are shown.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced and implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

The Catalyst 2948G is a fixed configuration switch. All ports are located on module 2; for this reason, if you enter *module-number*/*port-number* 1/*N*, an error message is displayed.

Examples

The following example shows how to display the flow-control port status and statistics:

```
Router# show port flowcontrol

Port    Send-Flowcontrol   Receive-Flowcntl   RxPause   TxPause
        Admin    Oper      Admin    Oper
-----   ----------------   ----------------   -------   ------
 3/1    on       disagree  on       disagree  0         0
 3/2    off      off       off      off       0         0
 3/3    desired  on        desired  off       10        10
```

Table 23 describes the fields shown in the display.

Table 23 show port flowcontrol Field Descriptions

Field	Description
Port	Module and port number.
Send-Flowcontrol Admin	Flow-control administration. Possible settings: • On indicates the local port sends flow control to the far end. • Off indicates the local port does not send flow control to the far end. • Desired indicates the local end sends flow control to the far end if the far end supports it.

Table 23 show port flowcontrol Field Descriptions (continued)

Field	Description
Send-Flowcontrol Oper	Flow-control operation. Possible settings: • Disagree indicates the two ports could not agree on a link protocol. • Off indicates that the local port cannot send flow control to a remote port.
Receive-Flowcntl Admin	Flow-control administration. Possible settings: • On indicates the local port requires the far end to send flow control. • Off indicates the local port does not allow the far end to send flow control. • Desired indicates the local end allows the far end to send flow control.
Receive-Flowcntl Oper	Flow-control operation. Possible settings: • Disagree indicates the two ports could not agree on a link protocol. • Off indicates that the local port cannot receive flow control from a remote port.
RxPause	Number of pause frames received.
TxPause	Number of pause frames transmitted.

Related Commands

Command	Description
set port flowcontrol	Sets the receive flow-control value for a particular Gigabit Ethernet switching module port.

show rep topology

To display Resilient Ethernet Protocol (REP) topology information for a segment or for all segments, including the primary and secondary edge ports in the segment, use the **show rep topology** command in privileged EXEC mode.

show rep topology [**segment** *segment-id*] [**archive**] [**detail**]

Syntax Description

segment *segment-id*	(Optional) The specific segment for which to display REP topology information. The ID range is from 1 to 1024.
archive	(Optional) Display the previous topology of the segment. This keyword can be useful for troubleshooting a link failure.
detail	(Optional) Display detailed REP topology information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(40)SE	This command was introduced.
12.2(33)SRC	Support was added for the Resilient Ethernet Protocol (REP) on the Cisco 7600 series router.
Cisco IOS XE Release 2.2	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Router.

Examples

The following is sample output from the **show rep topology segment** command for segment 1. The fields show in the display are self-explanatory.

```
Router# show rep topology segment 1

REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
sw1_multseg_3750 Gi1/1/1    Pri  Alt
sw3_multseg_3400 Gi0/13          Open
sw3_multseg_3400 Gi0/14          Alt
sw4_multseg_3400 Gi0/13          Open
sw4_multseg_3400 Gi0/14          Open
sw5_multseg_3400 Gi0/13          Open
sw5_multseg_3400 Gi0/14          Open
sw2_multseg_3750 Gi1/1/2         Open
sw2_multseg_3750 Gi1/1/1         Open
sw1_multseg_3750 Gi1/1/2    Sec  Open
```

This example shows output from the **show rep topology detail** command:

```
Router# show rep topology detail

REP Segment 2
repc_2_24ts, Fa0/2 (Primary Edge)
  Alternate Port, some vlans blocked
  Bridge MAC: 0019.e714.5380
```

```
  Port Number: 004
  Port Priority: 080
  Neighbor Number: 1 / [-10]
repc_3_12cs, Gi0/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 001
  Port Priority: 000
  Neighbor Number: 2 / [-9]
repc_3_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 3 / [-8]
repc_4_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a19d.7c80
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 4 / [-7]
repc_4_12cs, Gi0/2 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 001a.a19d.7c80
  Port Number: 002
  Port Priority: 040
  Neighbor Number: 5 / [-6]

<output truncated>
```

This example shows output from the **show rep topology segment archive** command:

```
Router# show rep topology segment 1 archive

REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
sw1_multseg_3750 Gi1/1/1    Pri  Open
sw3_multseg_3400 Gi0/13          Open
sw3_multseg_3400 Gi0/14          Open
sw4_multseg_3400 Gi0/13          Open
sw4_multseg_3400 Gi0/14          Open
sw5_multseg_3400 Gi0/13          Open
sw5_multseg_3400 Gi0/14          Open
sw2_multseg_3750 Gi1/1/2         Alt
sw2_multseg_3750 Gi1/1/1         Open
sw1_multseg_3750 Gi1/1/2    Sec  Open
```

Related Commands

Command	Description
rep segment	Enables REP on an interface and assigns a segment ID.

show spanning-tree

To display spanning-tree information for the specified spanning-tree instances, use the **show spanning-tree** command in privileged EXEC mode.

Cisco 2600, 3660, and 3845 Series Switches

show spanning-tree [*bridge-group*] [**active | backbonefast | blockedports | bridge | brief | inconsistentports | interface** *interface-type interface-number*| **root | summary** [**totals**] **| uplinkfast | vlan** *vlan-id*]

Cisco 6500/6000 Catalyst Series Switches and Cisco 7600 Series Routers

show spanning-tree [*bridge-group* **| active | backbonefast | bridge** [*id*] **| detail | inconsistentports | interface** *interface-type interface-number* [**portfast** [**edge**]] **| mst** [*list* **| configuration** [**digest**]] **| root | summary** [**totals**] **| uplinkfast | vlan** *vlan-id* **| port-channel** *number* **| pathcost** *method*]

Syntax Description

bridge-group	(Optional) Specifies the bridge group number. The range is 1 to 255.
active	(Optional) Displays spanning-tree information on active interfaces only.
backbonefast	(Optional) Displays spanning-tree BackboneFast status.
blockedports	(Optional) Displays blocked port information.
bridge	(Optional) Displays status and configuration of this switch.
brief	(Optional) Specifies a brief summary of interface information.
configuration [**digest**]	(Optional) Displays the multiple spanning-tree current region configuration.
inconsistentports	(Optional) Displays information about inconsistent ports.
interface *interface-type interface-number*	(Optional) Specifies the type and number of the interface. Enter each interface designator, using a space to separate it from the one before and the one after. Ranges are not supported. Valid interfaces include physical ports and virtual LANs (VLANs). See the "Usage Guidelines" for valid values.
list	(Optional) Specifies a multiple spanning-tree instance list.
mst	(Optional) Specifies multiple spanning-tree.
portfast [**edge**]	(Optional) Displays spanning-tree PortFast edge interface operational status. Beginning with Cisco IOS Release 12.2(33)SXI, the **edge** keyword is required. In earlier releases, the **edge** keyword is not used.
root	(Optional) Displays root-switch status and configuration.
summary	(Optional) Specifies a summary of port states.
totals	(Optional) Displays the total lines of the spanning-tree state section.
uplinkfast	(Optional) Displays spanning-tree UplinkFast status.
vlan *vlan-id*	(Optional) Specifies the VLAN ID. The range is 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094. If the *vlan-id* value is omitted, the command applies to the spanning-tree instance for all VLANs.

id	(Optional) Identifies the spanning tree bridge.
detail	(Optional) Shows status and configuration details.
port-channel *number*	(Optional) Identifies the Ethernet channel associated with the interfaces.
pathcost *method*	(Optional) Displays the default path-cost calculation method that is used. See the "Usage Guidelines" section for the valid values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(5.2)WC(1)	This command was integrated into Cisco IOS Release 12.0(5.2)WC(1).
12.1(6)EA2	This command was integrated into Cisco IOS Release 12.1(6)EA2. The following keywords and arguments were added: *bridge-group*, **active**, **backbonefast**, **blockedports**, **bridge**, **inconsistentports**, **pathcost** *method*, **root**, **totals**, and **uplinkfast**.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(15)ZJ	The syntax added in Cisco IOS Release 12.1(6)EA2 was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
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(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(4)T	The platform support and syntax added in Cisco IOS Release 12.2(15)ZJ was integrated into Cisco IOS Release 12.3(4)T.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs to 1–4094 for specified platforms.
12.2(33)SXI	This command was modified to require the **edge** keyword after **portfast**. The command output was modified to show the status of Bridge Assurance and PVST Simulation.

Usage Guidelines

The keywords and arguments that are available with the **show spanning-tree** command vary depending on the platform you are using and the network modules that are installed and operational.

Cisco 2600, 3660, and 3845 Series Switches

The valid values for **interface** *interface-type* are:

- **fastethernet**—Specifies a Fast Ethernet IEEE 802.3 interface.
- **port-channel**—Specifies an Ethernet channel of interfaces.

Cisco 6500/6000 Catalyst Switches and 7600 Series Routers

The **port-channel** *number* values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewal Services Module (FWSM) only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* 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 2 to 13 and valid values for the port number are from 1 to 48.

When checking spanning tree-active states and you have a large number of VLANs, you can enter the **show spanning-tree summary total** command. You can display the total number of VLANs without having to scroll through the list of VLANs.

The valid values for **interface** *interface-type* are:

- **fastethernet**—Specifies a Fast Ethernet IEEE 802.3 interface.
- **port-channel**—Specifies an Ethernet channel of interfaces.
- **atm**—Specifies an Asynchronous Transfer Mode (ATM) interface.
- **gigabitethernet**—Specifies a Gigabit Ethernet IEEE 802.3z interface.
- **multilink**—Specifies a multilink-group interface.
- **serial**—Specifies a serial interface.
- **vlan**—Specifies a catalyst VLAN interface.

The valid values for keyword **pathcoast** *method* are:

- **append**—Appends the redirected output to a URL (supporting the append operation).
- **begin**—Begins with the matching line.
- **exclude**—Excludes matching lines.
- **include**—Includes matching lines.
- **redirect**—Redirects output to a URL.
- **tee**—Copies output to a URL.

When you run the **show spanning-tree** command for a VLAN or an interface the switch router will display the different port states for the VLAN or interface. The valid spanning-tree port states are listening, learning, forwarding, blocking, disabled, and loopback. See Table 24 for definitions of the port states:

Table 24 show spanning-tree vlan Command Port States

Field	Definition
BLK	Blocked is when the port is still sending and listening to BPDU packets but is not forwarding traffic.
DIS	Disabled is when the port is not sending or listening to BPDU packets and is not forwarding traffic.
FWD	Forwarding is when the port is sending and listening to BPDU packets and forwarding traffic.
LBK	Loopback is when the port recieves its own BPDU packet back.
LIS	Listening is when the port spanning tree initially starts to listen for BPDU packets for the root bridge.
LRN	Learning is when the port sets the proposal bit on the BPDU packets it sends out

Examples

Cisco 2600, 3660, and 3845 Series Switches

The following example shows that bridge group 1 is running the VLAN Bridge Spanning Tree Protocol:

```
Router# show spanning-tree 1

Bridge group 1 is executing the VLAN Bridge compatible Spanning Tree Protocol
Bridge Identifier has priority 32768, address 0000.0c37.b055
Configured hello time 2, max age 30, forward delay 20
We are the root of the spanning tree
Port Number size is 10 bits
Topology change flag not set, detected flag not set
Times: hold 1, topology change 35, notification 2
      hello 2, max age 30, forward delay 20
Timers: hello 0, topology change 0, notification 0
  bridge aging time 300

Port 8 (Ethernet1) of Bridge group 1 is forwarding
   Port path cost 100, Port priority 128
   Designated root has priority 32768, address 0000.0c37.b055
   Designated bridge has priority 32768, address 0000.0c37.b055
   Designated port is 8, path cost 0
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 184, received 0
```

The following is sample output from the **show spanning-tree summary** command:

```
Router# show spanning-tree summary

UplinkFast is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN1                23       0         0        1          24
-------------------- -------- --------- -------- ---------- ----------
               1 VLAN 23       0         0        1          24
```

Table 25 describes the significant fields shown in the display.

Table 25 show spanning-tree summary Field Descriptions

Field	Description
UplinkFast	Indicates whether the spanning-tree UplinkFast feature is enabled or disabled.
Name	Name of VLAN.
Blocking	Number of ports in the VLAN in a blocking state.
Listening	Number of ports in a listening state.
Learning	Number of ports in a learning state.
Forwarding	Number of ports in a forwarding state.
STP Active	Number of ports using the Spanning-Tree Protocol.

The following is sample output from the **show spanning-tree brief** command:

```
Router# show spanning-tree brief

VLAN1
  Spanning tree enabled protocol IEEE
  ROOT ID     Priority 32768
              Address 0030.7172.66c4
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN1
  Spanning tree enabled protocol IEEE
  ROOT ID     Priority 32768
              Address 0030.7172.66c4
Port                            Designated
Name     Port ID Prio Cost Sts  Cost  Bridge ID      Port ID
-------- ------- ---- ---- ---  ----  -------------- -------
Fa0/11   128.17  128  100  BLK  38    0404.0400.0001 128.17
Fa0/12   128.18  128  100  BLK  38    0404.0400.0001 128.18
Fa0/13   128.19  128  100  BLK  38    0404.0400.0001 128.19
Fa0/14   128.20  128  100  BLK  38    0404.0400.0001 128.20
Fa0/15   128.21  128  100  BLK  38    0404.0400.0001 128.21
Fa0/16   128.22  128  100  BLK  38    0404.0400.0001 128.22
Fa0/17   128.23  128  100  BLK  38    0404.0400.0001 128.23
Fa0/18   128.24  128  100  BLK  38    0404.0400.0001 128.24
Fa0/19   128.25  128  100  BLK  38    0404.0400.0001 128.25
Fa0/20   128.26  128  100  BLK  38    0404.0400.0001 128.26
Fa0/21   128.27  128  100  BLK  38    0404.0400.0001 128.27

Port                            Designated
Name     Port ID Prio Cost Sts  Cost  Bridge ID      Port ID
-------- ------- ---- ---- ---  ----  -------------- -------
Fa0/22   128.28  128  100  BLK  38    0404.0400.0001 128.28
Fa0/23   128.29  128  100  BLK  38    0404.0400.0001 128.29
Fa0/24   128.30  128  100  BLK  38    0404.0400.0001 128.30 Hello Time   2 sec  Max Age 20
sec  Forward Delay 15 sec
```

Table 26 describes the significant fields shown in the display.

Table 26 show spanning-tree brief Field Descriptions

Field	Description
VLAN1	VLAN for which spanning-tree information is shown.
Spanning tree enabled protocol	Type of spanning tree (IEEE, IBM, CISCO).
ROOT ID	Indicates the root bridge.
Priority	Priority indicator.
Address	MAC address of the port.
Hello Time	Amount of time, in seconds, that the bridge sends bridge protocol data units (BPDUs).
Max Age	Amount of time, in seconds, that a BPDU packet should be considered valid.
Forward Delay	Amount of time, in seconds, that the port spends in listening or learning mode.
Port Name	Interface type and number of the port.
Port ID	Identifier of the named port.
Prio	Priority associated with the port.

Table 26 show spanning-tree brief Field Descriptions (continued)

Field	Description
Cost	Cost associated with the port.
Sts	Status of the port.
Designated Cost	Designated cost for the path.
Designated Bridge ID	Bridge identifier of the bridge assumed to be the designated bridge for the LAN associated with the port.

The following is sample output from the **show spanning-tree vlan 1** command:

```
Router# show spanning-tree vlan 1

Spanning tree 1 is executing the IEEE compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 00e0.1eb2.ddc0
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0010.0b3f.ac80
  Root port is 5, cost of root path is 10
  Topology change flag not set, detected flag not set, changes 1
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0

Interface Fa0/1  in Spanning tree 1 is down
   Port path cost 100, Port priority 128
   Designated root has priority 32768, address 0010.0b3f.ac80
Designated bridge has priority 32768, address 00e0.1eb2.ddc0
   Designated port is 1, path cost 10
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 0, received 0
```

Table 27 describes the significant fields shown in the display.

Table 27 show spanning-tree vlan Field Descriptions

Field	Description
Spanning tree	Type of spanning tree (IEEE, IBM, CISCO).
Bridge Identifier	Part of the bridge identifier and taken as the most significant part for bridge ID comparisons.
address	Bridge MAC address.
Root port	Identifier of the root port.
Topology change	Flags and timers associated with topology changes.

The following is sample output from the **show spanning-tree interface fastethernet0/3** command:

```
Router# show spanning-tree interface fastethernet0/3

Interface Fa0/3 (port 3) in Spanning tree 1 is down
   Port path cost 100, Port priority 128
   Designated root has priority 6000, address 0090.2bba.7a40
   Designated bridge has priority 32768, address 00e0.1e9f.4abf
   Designated port is 3, path cost 410
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 0, received 0
```

Cisco 6500/6000 Series Catalyst Switches and 7600 Series Routers

This example shows how to display a summary of interface information:

```
Router# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     0004.9b78.0800
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     0004.9b78.0800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Gi2/1            128.65           4 LIS         0  4097 0004.9b78.0800 128.65
Gi2/2            128.66           4 LIS         0  4097 0004.9b78.0800 128.66
Fa4/3            128.195         19 LIS         0  4097 0004.9b78.0800 128.195
Fa4/4            128.196         19 BLK         0  4097 0004.9b78.0800 128.195

Router#
```

Table 28 describes the fields that are shown in the example.

Table 28 show spanning-tree Command Output Fields

Field	Definition
Port ID Prio.Nbr	Port ID and priority number.
Cost	Port cost.
Sts	Status information.

This example shows how to display information about the spanning tree on active interfaces only:

```
Router# show spanning-tree active

UplinkFast is disabled
BackboneFast is disabled

 VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 0050.3e8d.6401
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 16384, address 0060.704c.7000
  Root port is 265 (FastEthernet5/9), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 18:13:54 ago
  Times:  hold 1, topology change 24, notification 2
          hello 2, max age 14, forward delay 10
  Timers: hello 0, topology change 0, notification 0

Router#
```

This example shows how to display the status of spanning-tree BackboneFast:

```
Router# show spanning-tree backbonefast

BackboneFast is enabled

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs)     : 0
Number of RLQ request PDUs received (all VLANs)   : 0
Number of RLQ response PDUs received (all VLANs)  : 0
Number of RLQ request PDUs sent (all VLANs)       : 0
Number of RLQ response PDUs sent (all VLANs)      : 0
Router#
```

This example shows how to display information about the spanning tree for this bridge only:

```
Router# show spanning-tree bridge

VLAN1
  Bridge ID  Priority    32768
             Address     0050.3e8d.6401
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
.
Router#
```

This example shows how to display detailed information about the interface:

```
Router# show spanning-tree detail

VLAN1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 4096, address 00d0.00b8.1401
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 9 last change occurred 02:41:34 ago
from FastEthernet4/21
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 1, topology change 0, notification 0, aging 300


Port 213 (FastEthernet4/21) of VLAN1 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.213.
Designated root has priority 4096, address 00d0.00b8.1401
Designated bridge has priority 4096, address 00d0.00b8.1401
Designated port id is 128.213, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 4845, received 1
Router#
```

This example shows how to display information about the spanning tree for a specific interface:

```
Router# show spanning-tree interface fastethernet 5/9

Interface Fa0/10 (port 23) in Spanning tree 1 is ROOT-INCONSISTENT
Port path cost 100, Port priority 128
Designated root has priority 8192, address 0090.0c71.a400
Designated bridge has priority 32768, address 00e0.1e9f.8940
```

This example shows how to display information about the spanning tree for a specific bridge group:

```
Router# show spanning-tree 1

UplinkFast is disabled
 BackboneFast is disabled

  Bridge group 1 is executing the ieee compatible Spanning Tree protocol
   Bridge Identifier has priority 32768, address 00d0.d39c.004d
   Configured hello time 2, max age 20, forward delay 15
   Current root has priority 32768, address 00d0.d39b.fddd
   Root port is 7 (FastEthernet2/2), cost of root path is 19
   Topology change flag set, detected flag not set
   Number of topology changes 3 last change occurred 00:00:01 ago
           from FastEthernet2/2
   Times:  hold 1, topology change 35, notification 2
           hello 2, max age 20, forward delay 15
   Timers: hello 0, topology change 0, notification 0  bridge aging time 15

Port 2 (Ethernet0/1/0) of Bridge group 1 is down

    Port path cost 100, Port priority 128
    Designated root has priority 32768, address 0050.0bab.1808
    Designated bridge has priority 32768, address 0050.0bab.1808
    Designated port is 2, path cost 0
    Timers: message age 0, forward delay 0, hold 0
    BPDU: sent 0, received 0
Router#
```

This example shows how to display a summary of port states:

```
Router# show spanning-tree summary

Root bridge for: Bridge group 1, VLAN0001, VLAN0004-VLAN1005
 VLAN1013-VLAN1499, VLAN2001-VLAN4094
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Platform PVST Simulation is enabled
Pathcost method used is long
Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
1 bridge               0        0         0        1          1
3584 vlans 3584 0 0 7168 10752


Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
Total                  3584     0         0        7169       10753
Router#
```

This example shows how to display the total lines of the spanning-tree state section:

```
Router#  show spanning-tree summary total

Root bridge for:Bridge group 10, VLAN1, VLAN6, VLAN1000.
Extended system ID is enabled.
PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
```

```
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is long

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
           105 VLANs 3433     0         0        105        3538

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs) :0
Number of inferior BPDUs received (all VLANs)     :0
Number of RLQ request PDUs received (all VLANs)   :0
Number of RLQ response PDUs received (all VLANs)  :0
Number of RLQ request PDUs sent (all VLANs)       :0
Number of RLQ response PDUs sent (all VLANs)      :0
Router#
```

This example shows how to display information about the spanning tree for a specific VLAN:

```
Router# show spanning-tree vlan 200

VLAN0200
 Spanning tree enabled protocol ieee
 Root ID Priority 32768
    Address 00d0.00b8.14c8
    This bridge is the root
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Bridge ID Priority 32768
    Address 00d0.00b8.14c8
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
    Aging Time 300
Interface Role Sts Cost Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4 Desg FWD 200000 128.196 P2p
Fa4/5 Back BLK 200000 128.197 P2p
Router#
```

Table 29 describes the fields that are shown in the example.

Table 29 show spanning-tree vlan Command Output Fields

Field	Definition
Role	Current 802.1w role; valid values are Boun (boundary), Desg (designated), Root, Altn (alternate), and Back (backup).
Sts	Spanning-tree states; valid values are BKN* (broken)[1], BLK (blocking), DWN (down), LTN (listening), LBK (loopback), LRN (learning), and FWD (forwarding).
Cost	Port cost.

Table 29 show spanning-tree vlan Command Output Fields (continued)

Field	Definition
Prio.Nbr	Port ID that consists of the port priority and the port number.
Status	Status information; valid values are as follows: • P2p/Shr—The interface is considered as a point-to-point (resp. shared) interface by the spanning tree. • Edge—PortFast has been configured (either globally using the **default** command or directly on the interface) and no BPDU has been received. • *ROOT_Inc, *LOOP_Inc, *PVID_Inc and *TYPE_Inc—The port is in a broken state (BKN*) for an inconsistency. The port would be (respectively) Root inconsistent, Loopguard inconsistent, PVID inconsistent, or Type inconsistent. • Bound(type)—When in MST mode, identifies the boundary ports and specifies the type of the neighbor (STP, RSTP, or PVST). • Peer(STP)—When in PVRST rapid-pvst mode, identifies the port connected to a previous version of the 802.1D bridge.

1. For information on the *, see the definition for the Status field.

This example shows how to determine if any ports are in the root-inconsistent state:

```
Router#  show spanning-tree inconsistentports

Name                 Interface            Inconsistency
-------------------- -------------------- ------------------
 VLAN1               FastEthernet3/1      Root Inconsistent

Number of inconsistent ports (segments) in the system :1
Router#
```

Related Commands

Command	Description
spanning-tree backbonefast	Enables BackboneFast on all Ethernet VLANs.
spanning-tree cost	Sets the path cost of the interface for STP calculations.
spanning-tree guard	Enables or disables the guard mode.
spanning-tree pathcost method	Sets the default path-cost calculation method.
spanning-tree portfast (interface configuration mode)	Enables PortFast mode.
spanning-tree portfast bpdufilter default	Enables BPDU filtering by default on all PortFast ports.
spanning-tree portfast bpduguard default	Enables BPDU guard by default on all PortFast ports.
spanning-tree port-priority	Sets an interface priority when two bridges vie for position as the root bridge.
spanning-tree uplinkfast	Enables UplinkFast.
spanning-tree vlan	Enables the STP on a VLAN.

show spanning-tree mst

To display the information about the Multiple Spanning Tree (MST) protocol, use the **show spanning-tree mst** command in privileged EXEC mode.

show spanning-tree mst [*instance-id-number* [**detail**] [*interface*] | **configuration** [**digest**] | **detail** | **interface** *interface* [**detail**]]

Syntax Description

instance-id-number	(Optional) Instance identification number; valid values are from 0 to 4094.
configuration	(Optional) Displays information about the region configuration.
digest	(Optional) Displays information about the Message Digest 5 (MD5) algorithm included in the current MST configuration identifier (MSTCI).
detail	(Optional) Displays detailed information about the MST protocol.
interface	(Optional) Displays information about the interface type; possible valid values for type are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, **ge-wan**, **port-channel**, and **vlan**.
interface	(Optional) Displays the information about the specific interface number. See the "Usage Guidelines" section for valid number values.

Command Modes

Privileged EXEC (#)

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.

Release	Modification
12.2(18)SXF	The changes are as follows: • The range of valid values for the *instance-id-number* changed to 0 to 4094. • The output of the **show spanning-tree mst configuration** command has changed as follows: – Displays the instance identification from 0 to 4094. – Displays the number of the currently configured instances from 0 to 65. – Adds the **digest** keyword to display the MD5 digest of the VLAN-to-instance mapping of the MST configuration. • The output of the **show spanning-tree mst detail** command has changed as follows: – The Regional Root field replaced the IST Master field. – The Internal Path field replaced the Path Cost field. – The Designated Regional Root field replaced the Designated IST Master field. – The txholdcount field was added in the Operational parameter line. • Displays new roles for all MST instances on the common and internal spanning tree (CIST) root port. • Displays the prestandard flag.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The valid values for *interface* 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 2 to 13 and valid values for the port number are from 1 to 48.

The number of valid values for **port-channel** *number* are a maximum of 64 values ranging from 1 to 282. The **port-channel** *number* values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewall Serices Module (FWSM) only.

The number of valid values for **vlan** are from 1 to 4094.

In the output display of the **show spanning-tree mst configuration** command, a warning message may display. This message appears if you do not map secondary VLANs to the same instance as the associated primary VLAN. The display includes a list of the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

In the output display of the **show spanning-tree mst configuration digest** command, if the output applies to both standard and prestandard bridges at the same time on a per-port basis, two different digests are displayed.

If you configure a port to transmit prestandard PortFast Bridge Protocol Data Units (BPDUs) only, the prestandard flag displays in the **show spanning-tree** commands. The variations of the prestandard flag are as follows:

- Pre-STD (or pre-standard in long format)—This flag displays if the port is configured to transmit prestandard BPDUs and if a prestandard neighbor bridge has been detected on this interface.
- Pre-STD-Cf (or pre-standard (config) in long format)—This flag displays if the port is configured to transmit prestandard BPDUs but a prestandard BPDU has not been received on the port, the autodetection mechanism has failed, or a misconfiguration, if there is no prestandard neighbor, has occurred.
- Pre-STD-Rx (or pre-standard (rcvd) in long format)—This flag displays when a prestandard BPDU has been received on the port but it has not been configured to send prestandard BPDUs. The port will send prestandard BPDUs, but we recommend that you change the port configuration so that the interaction with the prestandard neighbor does not rely only on the autodetection mechanism.

If the configuration is not prestandard compliant, for example, a single MST instance has an ID that is greater than or equal to 16, the prestandard digest is not computed and the following output is displayed:

```
Router# show spanning-tree mst configuration digest

Name      [region1]
Revision  2     Instances configured 3
Digest          0x3C60DBF24B03EBF09C5922F456D18A03
Pre-std Digest  N/A, configuration not pre-standard compatible
Router#
```

MST BPDUs include an MSTCI that consists of the region name, region revision, and an MD5 digest of the VLAN-to-instance mapping of the MST configuration.

See the **show spanning-tree** command for output definitions.

Examples

This example shows how to display information about the region configuration:

```
Router# show spanning-tree mst configuration

Name      [leo]
Revision  2702
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-9,11-19,21-29,31-39,41-4094
1         10,20,30,40
-------------------------------------------------------------------------------
```

This example shows how to display additional MST-protocol values:

```
Router# show spanning-tree mst 3 detail

###### MST03 vlans mapped: 3,3000-3999
Bridge address 0002.172c.f400 priority 32771 (32768 sysid 3)
Root this switch for MST03

GigabitEthernet1/1 of MST03 is boundary forwarding
Port info port id 128.1 priority 128
cost 20000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port
id 128.1
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 4, received 0
```

```
FastEthernet4/1 of MST03 is designated forwarding
Port info port id 128.193 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 254, received 1

FastEthernet4/2 of MST03 is backup blocking
Port info port id 128.194 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 252
Router#
```

This example shows how to display MST information for a specific interface:

```
Router# show spanning-tree mst 0 interface fastethernet 4/1 detail

Edge port: no (trunk) port guard : none
(default)
Link type: point-to-point (point-to-point) bpdu filter: disable
(default)
Boundary : internal bpdu guard : disable
(default)
FastEthernet4/1 of MST00 is designated forwarding
Vlans mapped to MST00 1-2,4-2999,4000-4094
Port info port id 128.193 priority 128 cost
200000
Designated root address 0050.3e66.d000 priority 8193
cost 20004
Designated ist master address 0002.172c.f400 priority 49152
cost 0
Designated bridge address 0002.172c.f400 priority 49152 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 492, received 3
Router#
```

This example shows how to display the MD5 digest included in the current MSTCI:

```
Router# show spanning-tree mst configuration digest

Name      [mst-config]
Revision  10    Instances configured 25
Digest          0x40D5ECA178C657835C83BBCB16723192
Pre-std Digest  0x27BF112A75B72781ED928D9EC5BB4251
Router#
```

This example displays the new master role for all MST instances at the boundary of the region on the port that is a CIST root port:

```
Router# show spanning-tree mst interface fastethernet4/9

FastEthernet4/9 of MST00 is root forwarding
Edge port: no             (default)        port guard : none        (default)
Link type: point-to-point (auto)           bpdu filter: disable     (default)
```

```
Boundary : boundary       (RSTP)           bpdu guard : disable     (default)
Bpdus sent 3428, received 6771

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- --------------------------------
0        Root FWD 200000    128.201  2-7,10,12-99,101-999,2001-3999,4001-4094
8        Mstr FWD 200000    128.201  8,4000
9        Mstr FWD 200000    128.201  1,9,100
11       Mstr FWD 200000    128.201  11,1000-2000
Router#
```

Related Commands

Command	Description
spanning-tree mst	Sets the path cost and port-priority parameters for any MST instance.
spanning-tree mst forward-time	Sets the forward-delay timer for all the instances on the Catalyst 6500 series switch.
spanning-tree mst hello-time	Sets the hello-time delay timer for all the instances on the Catalyst 6500 series switch.
spanning-tree mst max-hops	Specifies the number of possible hops in the region before a BPDU is discarded.
spanning-tree mst root	Designates the primary and secondary root, sets the bridge priority, and sets the timer value for an instance.

show spantree

To display spanning-tree information for a virtual LAN (VLAN) or port, use the **show spantree** command in privileged EXEC mode.

show spantree [*vlan*] [**active**]

show spantree *mod/port*

Syntax Description

vlan	(Optional) Number of the VLAN; valid values are from 1 to 1001 and from 1025 to 4094.
active	(Optional) Displays only the active ports.
mod/port	Number of the module and the port on the module. The slash mark is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on the 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 the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
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 you do not specify the VLAN number, VLAN 1 is displayed.

If you are in Multiple Instances of Spanning Tree (MISTP) mode, instance information is not displayed.

The maximum length of the channel port list is 47. The space in the Port(s) column might not be enough to display the entire list in one line. If this is the case, the port list is split into multiple lines. For example, in the following display, ports 6/5-8, 6/13, 6/15, 6/17, 6/19 are channeling:

```
.
.
.
Port(s)                  Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
6/5-8,6/13,6/15,6/17,6/1 1    not-connected 2684354   32   disabled 0

9
.
.
.
```

The Link Aggregation Control Protocol (LACP) for channels does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated).

The port is shown as "connected" if you use the **show port** command and as "not connected" if you use the **show spantree** command. This discrepancy occurs because the port is physically connected but never joined the active spanning-tree topology. To get the port to join the active spanning- tree topology, either set the duplex to full or set the channel mode to off for that port.

Examples

The following example shows how to display the active spanning tree port configuration for VLAN 1 while in Per VLAN Spanning Tree (PVST+ mode):

```
Router# (enable) show spantree 1 active

VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-60-70-4c-70-00
Designated Root Priority    16384
Designated Root Cost        19
Designated Root Port        2/3
Root Max Age   14 sec   Hello Time 2  sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32768
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 2/3                     1    forwarding           19   32 disabled 0
 2/12                    1    forwarding           19   32 disabled 0
```

The following example shows how to display the active spanning-tree port configuration for VLAN 1 (while in MISTP mode):

```
Router# (enable) show spantree 1 active

VLAN 1
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree enabled
VLAN mapped to MISTP Instance: 1
Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 2/3                     1    forwarding       200000   32 disabled 0
 2/12                    1    forwarding       200000   32 disabled 0
```

Table 30 describes the significant fields shown in the displays.

Table 30 show spantree Field Descriptions

Field	Description
VLAN	VLAN for which the spanning-tree information is shown.
Spanning tree mode	Indicates the current mode that spanning tree is operating in: • PVST—Per VLAN Spanning Tree • MSTP—Multiple Spanning Tree Protocol
Spanning tree type	Indicates the current Spanning Tree Protocol type: • IEEE—IEEE Spanning Tree • DEC—Digital Equipment Corporation Spanning Tree
Spanning tree enabled	Indicates whether Spanning Tree Protocol is enabled or disabled.
Designated Root	MAC address of the designated spanning-tree root bridge.
Designated Root Priority	Priority of the designated root bridge.
Designated Root Cost	Total path cost to reach the root.
Designated Root Port	Port through which the root bridge can be reached. (Shown only on nonroot bridges.)
Root Max Age	Amount of time a bridge packet data unit (BPDU) packet should be considered valid.
Hello Time	Number of times the root bridge sends BPDUs.
Forward Delay	Amount of time the port spends in listening or learning mode.
Port	Port number.
Vlan	VLAN to which the port belongs.
Port-State	Spanning tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent).
Cost	Cost associated with the port.
Prio	Priority associated with the port.
Portfast	Status of whether the port is configured to use the PortFast feature.
Channel_id	Channel ID number.

Related Commands

Command	Description
show spantree backbonefast	Displays whether the spanning-tree BackboneFast Convergence feature is enabled.
show spantree blockedports	Displays only the blocked ports on a per-VLAN or per-instance basis.
show spantree portvlancost	Shows the path cost for the VLANs or extended-range VLANs.
show spantree statistics	Shows spanning tree statistical information
show spantree summary	Displays a summary of spanning-tree information.
show spantree uplinkfast	Shows the UplinkFast feature settings.

show ssl-proxy module state

To display the spanning-tree state for the specified VLAN, enter the **show ssl-proxy module state** command in user EXEC mode.

show ssl-proxy module *mod* **state**

Syntax Description		
	mod	Module number.

Command Modes

User EXEC (>)

Command History

Release	Modification
12.2(18)SXD	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 supported on Cisco 7600 series routers that are configured with a Secure Sockets Layer (SSL) Services Module only.

Examples

This example shows how to verify that the VLAN information displayed matches the VLAN configuration. The fields shown in the display are self-explanatory.

```
Router# show ssl-proxy module 6 state

SSL-services module 6 data-port:
 Switchport:Enabled
Administrative Mode:trunk
Operational Mode:trunk
Administrative Trunking Encapsulation:dot1q
Operational Trunking Encapsulation:dot1q
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Trunking VLANs Enabled:100
Pruning VLANs Enabled:2-1001
Vlans allowed on trunk:100
Vlans allowed and active in management domain:100
Vlans in spanning tree forwarding state and not pruned:
100
Allowed-vlan :100
Router#
```

Related Commands

Command	Description
ssl-proxy module allowed-vlan	Adds the VLANs allowed over the trunk to the SSL Services Module.

show udld

To display the administrative and operational Unidirectional Link Detection Protocol (UDLD) status, use the **show udld** command in user EXEC mode.

show udld [*interface-id* | **neighbors**]

Syntax Description

interface-id	(Optional) Interface name and number.
neighbors	(Optional) Displays neighbor information only.

Command Modes

User EXEC (>)

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(18)SXD	This command was changed to include the **neighbors** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you do not enter an *interface-id* value, the administrative and operational UDLD status for all interfaces are displayed.

Examples

This example shows how to display the UDLD state for a single interface. The fields shown in the display are self-explanatory.

```
Router# show udld gigabitethernet2/2

Interface Gi2/2
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement
Message interval: 60
Time out interval: 5
No multiple neighbors detected
    Entry 1
    ---
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
```

```
    Device name: 0050e2826000
    Port ID: 2/1
    Neighbor echo 1 device: SAD03160954
    Neighbor echo 1 port: Gi1/1

    Message interval: 5
    CDP Device name: 066527791
Router#
```

This example shows how to display neighbor information only. The fields shown in the display are self-explanatory.

```
Router# show udld neighbors

Port     Device Name                    Device ID    Port-ID OperState
-------- ------------------------------ ------------ ------- --------------
Gi3/1    SAL0734K5R2                    1            Gi4/1   Bidirectional
Gi4/1    SAL0734K5R2                    1            Gi3/1   Bidirectional
Router#
```

Related Commands

Command	Description
udld	Enables aggressive or normal mode in UDLD and sets the configurable message time.
udld port	Enables UDLD on the interface or enables UDLD in aggressive mode on the interface.

show vlan

To display VLAN information, use the **show vlan** command in privileged EXEC mode.

show vlan [**brief** | **id** *vlan-id* | **name** *name* [**ifindex**] | **ifindex**]

Syntax Description

brief	(Optional) Displays only a single line for each VLAN, naming the VLAN, status, and ports.
id *vlan-id*	(Optional) Displays information about a single VLAN that is identified by a VLAN ID number; valid values are from 1 to 4094.
name *name*	(Optional) Displays information about a single VLAN that is identified by VLAN name; valid values are an ASCII string from 1 to 32 characters.
ifindex	(Optional) Displays the VLAN's ifIndex number.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Each Ethernet switch port and Ethernet repeater group belong to only one VLAN. Trunk ports can be on multiple VLANs.

If you shut down a VLAN using the **state suspend** or the **state active** command, these values appear in the Status field:

- suspended—VLAN is suspended.
- active—VLAN is active.

If you shut down a VLAN using the **shutdown** command, these values appear in the Status field:

- act/lshut—VLAN status is active but shut down locally.
- sus/lshut—VLAN status is suspended but shut down locally.

This is an example of the ouput for a VLAN (VLAN0002) that is active but shut down locally:

```
Router# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    VLAN0002                         act/lshut Fa5/9
<...Output truncated...>
```

If a VLAN is shut down internally, these values appear in the Status field:

- act/ishut—VLAN status is active but shut down internally.
- sus/ishut—VLAN status is suspended but shut down internally.

This is an example of the ouput for a VLAN (VLAN0002) that is active but shut down internally:

```
Router# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    VLAN0002                         act/ishut Fa5/9
<...Output truncated...>
```

If a VLAN is shut down locally and internally, the value that is displayed in the Status field is act/ishut or sus/ishut. If a VLAN is shut down locally only, the value that is displayed in the Status field is act/lshut or sus/lshut.

Separate VLAN ranges with a hyphen, and separate VLANs with a comma and no spaces in between. For example, you can enter the following:

```
Router# show vlan id 1-4,3,7,5-20
```

Examples

This example shows how to display the VLAN parameters for all VLANs within the administrative domain:

```
Router# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    VLAN0002                         active    Fa5/9
3    VLAN0003                         active    Fa5/9
4    VLAN0004                         active    Fa5/9
5    VLAN0005                         active    Fa5/9
6    VLAN0006                         active    Fa5/9
<...Output truncated...>

1004 fddinet-default                  active    Fa5/9
1005 trbrf-default                    active    Fa5/9

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        303    0
4    enet  100004     1500  -      -      -        -    -        304    0
5    enet  100005     1500  -      -      -        -    -        305    0
6    enet  100006     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0

<...Output truncated...>

Remote SPAN VLANs
-----------------
2, 20

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
Router#
```

This example shows how to display the VLAN name, status, and associated ports only:

```
Router# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    VLAN0002                         active    Fa5/9
3    VLAN0003                         act/lshut Fa5/9
4    VLAN0004                         act/lshut Fa5/9
5    VLAN0005                         active    Fa5/9
10   VLAN0010                         active    Fa5/9
.
.
.
999  VLAN0999                         active    Fa5/9
1002 fddi-default                     active    Fa5/9
1003 trcrf-default                    active    Fa5/9
1004 fddinet-default                  active    Fa5/9
1005 trbrf-default                    active    Fa5/9
Router#
```

This example shows how to display the VLAN parameters for multiple VLANs:

```
Router# show vlan id 1-4,3,7,5-20

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/7, Fa5/12
2    VLAN0002                         active
3    VLAN0003                         act/lshut
4    VLAN0004                         act/lshut
5    VLAN0005                         active
6    VLAN0006                         active
10   VLAN0010                         active
20   VLAN0020                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        303    0
4    enet  100004     1500  -      -      -        -    -        304    0
5    enet  100005     1500  -      -      -        -    -        305    0
6    enet  100006     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Router#
```

This example shows how to display the ifIndex number for VLAN 10 only:

```
Router# show vlan id 10 ifindex

 VLAN Ifindex
 ---- -------
 10   37
Router#
```

Table 31 describes the fields that are shown in the example.

Table 31 show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend, act/lshut or sus/lshut, or act/ishut or sus/ishut).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type that is used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are SRB and SRT; the default is SRB.
AREHops	Maximum number of hops for All-Routes Explorer frames—possible values are 1 through 13; the default is 7.
STEHops	Maximum number of hops for Spanning Tree Explorer frames—possible values are 1 through 13; the default is 7.
Backup CRF	Status of whether the TrCRF is a backup path for traffic.
Ifindex	Number of the ifIndex.
Remote SPAN VLAN	RSPAN status.
Primary	Number of the primary VLAN.
Secondary	Number of the secondary VLAN.
Ports	Indicates the ports within a VLAN.
Type	Type of VLAN—Possible values are primary, isolated, community, nonoperation, or normal.

Related Commands

Command	Description
show vlan private-vlan	Display PVLAN information.
vlan (config-VLAN submode)	Configures a specific VLAN.
vtp	Configures the global VTP state.

show vlan access-log config

To display VLAN access control list (VACL) logging configuration properties, use the **show vlan access-log config** command in privileged EXEC mode.

show vlan access-log config

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Syslog messages are generated when the device reaches the set threshold, or five minutes after the previous message is displayed, whichever occurs first. The threshold controls the rate of the syslog message only and does not affect the log table entries. Packets exceeding the specified rate limit will not be logged.

Examples

The following example shows how to display the configured VACL logging properties. The fields are self-explanatory.

```
Router# show vlan access-log config

VACL Logging Configuration:
        max log table size     :500
        log threshold          :4000
        rate limiter           :3000
```

Related Commands

Command	Description
show vlan access-log flow	Displays the contents of the VACL flow table.
show vlan access-log statistics	Displays packets, message counts, and other statistics of the VACL.
vlan access-log	Configures VACL logging properties, including the log-table size, redirect-packet rate, and logging threshold.

show vlan access-log flow

To display VLAN access control list (VACL) flow table contents, use the **show vlan access-log flow** command in privileged EXEC mode.

show vlan access-log flow *protocol* {*src-addr src-mask* | **any** | **host** {*hostname* | *host-ip*}} {*dst-addr dst-mask* | **any** | **host** {*hostname* | *host-ip*}} [**vlan** *vlan-id*]

Syntax Description

protocol	Protocol name or number; valid values are **icmp**, **igmp**, **ip**, **tcp**, **udp**, or numbers from 0 to 255 to designate a protocol.
src-addr src-mask	Source address and mask.
any	Displays information for any host.
host *hostname*	Displays information for a hostname.
host *host-ip*	Displays information for a host IP address.
dst-addr dst-mask	Destination address and mask.
vlan *vlan-id*	(Optional) Displays information for a specific VLAN valid value. Range is from 1 to 4094.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Entries for the standard protocols or any protocol can be displayed by specifying the protocol name or protocol number. Entries are removed from the table, if there is no increment in the packet counter after the last syslog message.

Examples

The following example shows how to display the VACL flow table contents.

```
Router# show vlan access-log flow 17 172.20.10.110 255.255.0.0 172.20.10.105 255.255.0.0

id  prot    src_ip          dst_ip      sport  dport vlan    port    count   total
lastlog

-------------------------------------------------------------------------------
1  17   172.20.10.110   172.20.10.105    68    67   2    Gi1/0/3    324    325
00:03:14.338
2  17   172.20.10.109   172.20.10.105    68    67   2    Gi1/0/3    324    325
00:03:13.843
3  17   172.20.10.108   172.20.10.105    68    67   2    Gi1/0/3    325    326
00:03:13.340
4  17   172.20.10.107   172.20.10.105    68    67   2    Gi1/0/3    326    327
00:03:12.845
5  17   172.20.10.106   172.20.10.105    68    67   2    Gi1/0/3    327    328
00:03:12.342
6  17   172.20.10.110   172.20.10.105    68    67   2    Gi1/0/2    603    604
00:02:32.202
7  17   172.20.10.109   172.20.10.105    68    67   2    Gi1/0/2    605    606
00:02:31.204
8  17   172.20.10.108   172.20.10.105    68    67   2    Gi1/0/2    607    608
00:02:30.206
9  17   172.20.10.107   172.20.10.105    68    67   2    Gi1/0/2    607    608
00:02:29.216
10  17   172.20.10.106   172.20.10.105    68    67  2    Gi1/0/2    607    608
00:02:28.201

Total number of matched entries: 10
```

Table 32 describes the significant fields shown in the display.

Table 32 show vlan access-log flow Field Descriptions

Field	Description
prot	Protocol number.
src_ip	Source IP address.
dst_ip	Destination IP address.
sport	Source port.
dport	Destination port.
vlan	VLAN on which the packet arrived.
port	Physical interface on which the packet arrived.
count	Indicates the number of packets generated since the last syslog message was generated.
total	Cumulative count of packets for the flow.
lastlog	Time stamp of the last log.

Related Commands

Command	Description
show vlan access-log config	Displays VACL logging configuration properties.
show vlan access-log statistics	Displays packets, message counts, and other statistics of the VACL.
vlan access-log	Configures VACL logging properties, including the log-table size, redirect-packet rate, and logging threshold.

show vlan access-log statistics

To display VLAN access control list (VACL) packet counts, messages, and other statistics, use the **show vlan access-log statistics** command in privileged EXEC mode.

show vlan access-log statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

All platforms do not display VACL logging index. Packets that are dropped do not generate any syslog messages.

Examples

The following example shows how to display the VACL statistics. The fields are self-explanatory.

```
Router# show vlan access-log statistics

VACL Logging Statistics:
        total packets          :0
        logged                 :0
        dropped                :0
Dropped Packets Statistics:
        unsupported protocol   :0
        no packet buffer       :0
        hash queue full        :0
        flow table full        :0
Misc Information:
        VACL Logging LTL Index :0x7E02
        free packet buffers    :8192
        log messages sent      :0
        log table size         :0
```

Related Commands

Command	Description
show vlan access-log config	Displays VACL logging configuration properties.
show vlan access-log flow	Displays the contents of the VACL flow table.
vlan access-log	Configures VACL logging properties, including the log-table size, redirect-packet rate, and logging threshold.

show vlan access-map

To display the contents of a VLAN-access map, use the **show vlan access-map** command in privileged EXEC mode.

show vlan access-map [*map-name*]

Syntax Description

map-name	(Optional) VLAN access-map name.

Command Modes

Privileged EXEC (#)

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.

Examples

This command shows how to display the contents of a VLAN-access map. The fields shown in the display are self-explanatory.

```
Router# show vlan access-map access_map_example_1

Vlan access-map access_map_example_1
        match: ip address 13
        action: forward capture
```

Related Commands

Command	Description
action	Sets the packet action clause.
match	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
vlan access-map	Creates a VLAN access map or enters VLAN access-map command mode.

show vlan all-ports

To display VLAN information for trunk and access ports, use the **show vlan all-ports** command in privileged EXEC mode.

show vlan all-ports

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display VLAN information for trunk and access ports:

```
Router# show vlan all-ports

VLAN Name Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    VLAN0002                         active
3    VLAN0003                         active
.
.
.
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                      act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        303    0
.
.
.
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 trcrf 101003     4472  1005   3276   -        -    srb      0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trbrf 101005     4472  -      -      15       ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1005 trbrf 101005     4472  -      -      15       ibm  -        0      0


VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
802  0       0       off
1003 7       7       off
```

```
Primary Secondary Type            Ports
------- --------- ----------------- ------------------------------------------
```

Table 33 describes the significant fields shown in the display.

Table 33 show vlan all-ports Field Descriptions

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BridgeNo	Bridge number for the VLAN, if applicable.
Stp	Spanning-Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—Possible values are source-route bridging (SRB) and source-route transparent bridging (SRT); the default is SRB.
Trans1, Trans2	Types of translational bridges that the VLAN in the VLAN column is configured to translate to. Translational bridge VLANs must be a VLAN media type different from the affected VLAN; if two VLANs are specified, each one must be a different type. Common VLAN types include Ethernet (enet), FDDI (fdnet), and Token Ring (tnet). The numbers in the "Trans1" and "Trans2" columns refer to the VLAN ID numbers of the translational bridge VLANs. **Note** The term "VLAN translation" is also used in Cisco configuration guides for mapping specific VLANs in a given trunk to another VLAN that is of the same media type. In this context the term "VLAN translation" refers to a form of VLAN mapping that is using the term "VLAN translation" to describe it.
AREHops	Number of All Route Explorer (ARE) hops.
STEHops	Number of Spanning-Tree Explorer (STE) hops.
Backup CRF	Status of the backup Concentrator relay function (CRF).
primary	Primary VLAN.
secondary	Secondary VLAN.

show vlan counters

To display the software-cached counter values, use the **show vlan counters** command in privileged EXEC mode.

show vlan [**id** *vlanid*] **counters**

Syntax Description

id *vlanid*	(Optional) Displays the software-cached counter values for a specific VLAN; valid values are from 1 to 4094.

Command Modes

Privileged EXEC (#)

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 introduced.
12.2(50)SY	This command was introduced. Command output was updated to count broadcast packets with Unicast counters.

Usage Guidelines

The **show vlan id counters** command is not supported on switch virtual interfaces (SVIs).

For Layer 2 and Layer 3 VLAN interfaces and router ports, per-interface switching statistics and VLAN-counter information to the Multilayer Switching Feature Card 2 (MSFC2) are exported approximately every 3 minutes.

If you enter the **show vlan counters** command with no arguments, the software-cached counter values for all VLANs are displayed.

Examples

This example shows how to display the software-cached counter values for a specific VLAN. The fields shown in the display are self-explanatory.

```
Router# show vlan id 205 counters

VLAN vlanid 205
L2-Unicast-Pkts      10
L3-In-Unicast-Pkts   0
L3-Out-Unicast-Pkts  0
L2-NonUnicast-Pkts + L3-In-NonUnicast-Pkts  5
L3-Out-NonUnicast-Pkts   6
L2-Unicast-Octets 6
L3-In-Unicast-Octets 6
L3-Out-Unicast-Octets 6
L2-NonUnicast-Octets + L3-In-NonUnicast-Octets 6
L3-Out-NonUnicast-Octets 6
Router#
```

Related Commands

Command	Description
clear vlan counters	Clears the software-cached counter values to zero for a specified VLAN or all existing VLANs.

show vlan dot1q tag native

To display native VLAN-tagging information, use the **show vlan dot1q tag native** command in privileged EXEC mode.

show vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

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.

Examples

This example shows how to display native VLAN-tagging information. The fields shown in the display are self-explanatory.

```
Router# show vlan dot1q tag native

dot1q native vlan tagging is enabled
Internal dot1q native vlan: 1015

Router#
```

Related Commands

Command	Description
vlan dot1q tag native	Enables dot1q tagging for all VLANs in a trunk.

show vlan filter

To display information about the VLAN filter, use the **show vlan filter** command in privileged EXEC mode.

show vlan filter [**access-map** *map-name* | **vlan** *vlan-id* | **interface** *interface interface-number*]

Syntax Description

access-map *map-name*	(Optional) Displays the VLANs that are filtered by the specified map.
vlan *vlan-id*	(Optional) Displays the filter for the specified VLAN; valid values are from 1 to 4094.
interface *interface*	(Optional) Specifies the interface type; valid values are **pos**, **atm**, or **serial**. See the "Usage Guidelines" section for additional information.
interface-number	(Optional) Interface number; see the "Usage Guidelines" section for additional information.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

The **show vlan filter** *map-name* **interface** command accepts only ATM, packet over SONET/SDH (POS), or serial interface types. If your system is not configured with any of these interface types, the **interface** *interface interface-number* keyword and arguments are not provided.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* 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 2 to 13 and valid values for the port number are from 1 to 48.

If you do not specify an optional keyword and argument, all mappings are displayed. If you enter **access-map** *map_name*, all the VLANs and interfaces that are associated with the specified map are shown. If you enter **vlan** *vlan-id* or **interface** *interface interface-number*, its associated access map, if existing, is shown.

In the output for VLAN access control lists (VACLs) on VLANs, the following applies:

- Configured on VLANs—User configured
- Active on VLANs—VLAN list on which the VACL is active

In the WAN-interface outputs, the following applies:

- Configured on interfaces—User configured
- Active on Interfaces—Interfaces on which the VACL is active

Examples

This example shows how to display mappings between the VACLs and the VLANs and the VACLs and the interfaces. The fields shown in the display are self-explanatory.

```
Router# show vlan filter

VLAN Map mordred:
   Configured on VLANs: 2,4-6
   Active on VLANs: 2,4-6
Router#
```

Related Commands

Command	Description
vlan access-map	Creates a VLAN access map or enters VLAN access-map command mode.
vlan filter	Applies a VLAN access map.

show vlan free

To display the total number of free VLANs on a router, use the **show vlan free** command in privileged EXEC mode.

show vlan free

Syntax Description

This command has no arguments or keywords.

Command Default

All free VLANs are displayed.

Command Modes

Privileged EXEC (#)

Usage Guidelines

The **show vlan free** command displays the total number of free VLANs on a router.

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

The following is sample output from the **show vlan free** command. This example lists the number of free VLANs on a router. The fields shown in the display are self-explanatory.

```
Router# show vlan free

Free VLANs
----------
2
3
4
5
6
7
8
9
10
```

Related Commands

Command	Description
show vlan	Displays the VLAN information in the system.

show vlan free summary

To display the usage summary information for VLANs, use the **show free vlan summary** command in privileged EXEC mode.

show vlan free summary

Syntax Description

This command has no arguments or keywords.

Command Default

Usage summary information for all of the free VLANs is displayed.

Command Modes

Privileged EXEC (#)

Usage Guidelines

The **show vlan free summary** command displays the following VLAN information:

- Total number of available VLANs
- Total number of free VLANs
- Total number of used VLANs.

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to view the summary information for the existing VLANs in the system. The field descriptions shown in the display are self-explanatory.

```
Router# show vlan free summary

======= vlan free/usage Summary =======

Total number of available vlans = 4094

Total number of free vlans = 4074

Total number of used vlans = 20

Router#
```

Related Commands

Command	Description
show vlan free	Displays the total number of the free VLANs on a router.

show vlan internal usage

To display information about the internal VLAN allocation, use the **show vlan internal usage** command in privileged EXEC mode.

show vlan [**id** *vlan-id*] **internal usage**

Syntax Description

id *vlan-id*	(Optional) Displays information about the internal VLAN allocation for the specified VLAN; valid values are from 1 to 4094.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

In some cases, the output displays the following:

```
workaround vlan
```

A workaround VLAN is used to enable the Policy Feature Card (PFC)-based policing on the PWAN1 main interface. Without the workaround VLAN, the packets hit the PFC policer twice for PWAN1 because the same VLAN is used when packets traverse the local bus before and after Parallel eXpress Forwarding (PXF) processing.

Entering the **show vlan internal usage** command displays the Optical Services Module (OSM) interfaces and subinterfaces in addition to the regular Ethernet interfaces.

To display the associated subinterfaces, enter the **show cwan vlan** command. The **show cwan vlan** command displays the mapping between the WAN subinterface and the internal VLANs in use.

Examples

This example shows how to display the current internal VLAN allocation. The fields shown in the displays are self-explanatory.

```
Router# show vlan internal usage

VLAN Usage
---- --------------------
1025 -
1026 -
1027 -
1028 -
1029 Port-channel6
1030 GigabitEthernet1/2
1032 FastEthernet3/20
1033 FastEthernet3/21
1129 -
```

This example shows how to display the internal VLAN allocation for a specific VLAN:

```
Router# show vlan id 1030 internal usage

VLAN Usage
---- --------------------
1030 GigabitEthernet1/2
```

show vlan mapping

To register a mapping of an 802.1Q VLAN to an Inter-Switch Link (ISL) VLAN, use the **show vlan mapping** command in privileged EXEC mode.

show vlan mapping

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

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.

Examples

This example shows how to list the map for an 802.1Q VLAN to an ISL VLAN. The fields shown in the display are self-explanatory.

```
Router# show vlan mapping

802.1Q Trunk Remapped VLANs:
802.1Q VLAN ISL VLAN
----------- -----------
101         202
200         330
Router#
```

Related Commands

Command	Description
show interfaces vlan mapping	Displays the status of a VLAN mapping on a port.
switchport vlan mapping enable	Enables VLAN mapping per switch port.

show vlan port provisioning

To display the VLAN port provisioning status, use the **show vlan port provisioning** command in privileged EXEC mode.

show vlan port provisioning

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display the VLAN port provisioning status. The fields shown in the display are self-explanatory.

```
Router# show vlan port provisioning

port provision: disabled
```

Related Commands

Command	Description
vlan port provisioning	Enables or disables VLAN port provisioning.

show vlan private-vlan

To display private VLAN (PVLAN) information, use the **show vlan private-vlan** command in privileged EXEC mode.

show vlan private-vlan [**type**]

Syntax Description

type	(Optional) Displays the PVLAN type (isolated, community, or primary).

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

In the **show vlan private-vlan type** command output display, "normal" displayed as a type indicates a regular VLAN that is configured in a PVLAN. A display of "normal" means that two VLANs have been associated before the type was set and that the PVLAN is not operational. This information is useful for debugging purposes.

Examples

This example shows how to display information about all currently configured PVLANs:

```
Router# show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
2       301       community         Fa5/3, Fa5/25
2       302       community
        10        community
100     101       isolated
150     151       non-operational
        202       community
        303       community
401     402       non-operational
Router#
```

This example shows how to display information about all currently configured PVLAN types:

```
Router# show vlan private-vlan type

Vlan Type
---- -----------------
202  primary
303  community
304  community
305  community
306  community
```

```
307  community
308  normal
309  community
440  isolated
Router#
```

Table 34 describes the fields that are shown in the example.

Table 34 show vlan private-vlan Command Output Fields

Field	Description
Primary	Number of the primary VLAN.
Secondary	Number of the secondary VLAN.
Secondary-Type	Secondary VLAN type—Possible values are isolated or community.
Ports	Indicates the ports within a VLAN.
Type	Type of VLAN—Possible values are primary, isolated, community, nonoperation, or normal.

Related Commands

Command	Description
private-vlan mapping	Creates a mapping between the primary and the secondary VLANs so that both VLANs share the same primary VLAN SVI.
private-vlan	Configures PVLANs and the association between a PVLAN and a secondary VLAN.

show vlan remote-span

To display a list of remote Switched Port Analyzer (RSPAN) VLANs, use the **show vlan remote-span** command in privileged EXEC mode.

show vlan remote-span

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

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.

Examples

This example shows how to display a list of remote SPAN VLANs. The fields shown in the display are self-explanatory.

```
Router# show vlan remote-span

Remote SPAN VLANs
------------------------------------------------------------------------------
2,20
```

Related Commands

Command	Description
remote-span	Configures a VLAN as an RSPAN VLAN.
vlan (config-VLAN submode)	Configures a specific VLAN.

show vlan virtual-port

To display the number of logical virtual ports required, use the **show vlan virtual-port** command in privileged EXEC mode.

show vlan virtual-port [**slot** *number*]

Syntax Description

slot *number*	(Optional) Specifies the slot number of which status is to be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the number of logical virtual ports that are required for a specific slot. The fields shown in the display are self-explanatory.

```
Router# show vlan virtual-port slot 3

Slot 3
Port        Virtual-ports
------------------------
Fa3/1             1
Fa3/2             1
Fa3/3             1
Fa3/4             1
Fa3/5             1
Fa3/6             1
Fa3/7             1
Fa3/8             1
Fa3/11            1
Fa3/12            1
Fa3/13            1
.
.
.
Fa3/33            4
Fa3/34            4
Fa3/35            4
Fa3/36            4
Fa3/37            4
Fa3/38            4
Fa3/39            4
Fa3/40            4
Total virtual ports:82
Router#
```

This example shows how to display the number of logical virtual ports that are required for all slots. The fields shown in the display are self-explanatory.

```
Router# show vlan virtual-port

Slot 1
-------
Total slot virtual ports 1
Slot 3
-------
Total slot virtual ports 82
Slot 4
-------
Total slot virtual ports 4
Total chassis virtual ports 87
Router#
```

show vlan-range

To display the VLAN range, use the **show vlan-range** command in privileged EXEC mode.

show vlan-range

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show vlan-range** command. The field descriptions in the display are self-explanatory.

```
Router# show vlan-range

IDB-less VLAN Ranges on FastEthernet0/1 (1 ranges)
7-67                                    (range)
```

Related Commands

Command	Description
vlan-range dot1q	Enables IEEE 802.1Q VLAN encapsulation for a range of VLANs on Ethernet interface.

show vlans

To display VLAN subinterfaces, use the **show vlans** command in privileged EXEC mode.

show vlans

Catalyst 6500 Series Switches and Cisco 7600 Series Routers

show vlans [*vlan*]

Syntax Description

vlan	(Optional) VLAN ID number; valid values are from 1 to 4094.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.1(3)T	This command was modified to display traffic count on FastEthernet subinterfaces.
12.1(7)E	This command was integrated into Cisco IOS Release 12.1(7)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

On the Catalyst 6500 series switches and Cisco 7600 series routers, the EXEC **show vlan** command displays information about the Layer 2 VLAN. The privileged EXEC **show vlans** command displays information about the VLAN subinterface in Layer 3.

When entering the **show vlans** command, you cannot shorten the **vlans** keyword.

If you want to view the Layer 3 statistics, do not use the **show vlans** command, instead use the **show interface vlan** *vlan-num* **stats** command or the **show interface vlan** *vlan-num* **accounting** command.

Examples

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

```
Router# show vlans

Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interface:   FastEthernet5/0.1

    Protocols Configured:   Address:              Received:        Transmitted:
            IP              10.0.0.3                    16               92129

Virtual LAN ID:  3 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interface:   Ethernet6/0/1.1
```

```
    Protocols Configured:   Address:              Received:        Transmitted:
            IP              10.0.0.5                  1558                1521

Virtual LAN ID:  4 (Inter Switch Link Encapsulation)

    vLAN Trunk Interface:   FastEthernet5/0.2

    Protocols Configured:   Address:              Received:        Transmitted:
            IP              10.0.0.7                     0                   7
```

The following is sample output from the **show vlans** command indicating a native VLAN and a bridged group:

```
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet1/0/2
```

This example shows how to display information about the Cisco IOS VLAN subinterfaces:

```
Router# show vlans

Virtual LAN ID: 122 (Inter Switch Link Encapsulation)
VLAN Trunk Interface:  GE-WAN9/1.1
Protocols Configured:  Address:             Received:       Transmitted:
           IP              10.122.0.2                  18                  16
Virtual LAN ID: 123 (Inter Switch Link Encapsulation)
VLAN Trunk Interface:  GE-WAN9/1.2
Protocols Configured:  Address:             Received:       Transmitted:
           IP              10.123.0.2                  13                  16
Virtual LAN ID: 124 (Inter Switch Link Encapsulation)
VLAN Trunk Interface:  GE-WAN9/1.3
Protocols Configured:  Address:             Received:       Transmitted:
           IP              10.124.0.2                   0                  17
Virtual LAN ID: 133 (Inter Switch Link Encapsulation)
VLAN Trunk Interface:  GE-WAN9/3.1
Protocols Configured:  Address:             Received:       Transmitted:
           IP              10.133.0.1                   0                   1
Virtual LAN ID: 134 (Inter Switch Link Encapsulation)
VLAN Trunk Interface:  GE-WAN9/3.2
Protocols Configured:  Address:             Received:       Transmitted:
           IP              10.134.0.1                   0                   1
```

This VLAN is configured as a native VLAN for the following interfaces:

```
FastEthernet1/0/2

   Protocols Configured:   Address: Received:        Transmitted:

Virtual LAN ID:  100 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet1/0/2.1

   Protocols Configured:   Address: Received:        Transmitted:

        Bridging        Bridge Group 1 0                   0
```

The following is sample output from the **show vlans** command that shows the traffic count on Fast Ethernet subinterfaces:

```
Router# show vlans

Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)
```

```
    vLAN Trunk Interface:   FastEthernet5/0.1

    Protocols Configured:   Address:              Received:        Transmitted:
           IP               172.16.0.3                   16              92129

Virtual LAN ID:  3 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interface:   Ethernet6/0/1.1

    Protocols Configured:   Address:              Received:        Transmitted:
           IP               172.20.0.3                 1558               1521

Virtual LAN ID:  4 (Inter Switch Link Encapsulation)

    vLAN Trunk Interface:   FastEthernet5/0.2

    Protocols Configured:   Address:              Received:        Transmitted:
           IP               172.30.0.3                    0                  7
```

Table 35 describes the significant fields shown in the display.

Table 35 show vlans Field Descriptions

Field	Description
Virtual LAN ID	Domain number of the VLAN.
vLAN Trunk Interface	Subinterface that carries the VLAN traffic.
Protocols Configured	Protocols configured on the VLAN.
Address	Network address.
Received	Number of packets received.
Transmitted	Number of packets sent.

Related Commands

Command	Description
vlan database	Enters VLAN configuration mode.
vlan (VLAN)	Configures a specific VLAN.

show vlans dot1q

To display statistics about 802.1Q VLAN subinterfaces, use the **show vlans dot1q** command in privileged EXEC mode.

show vlans dot1q [**internal** | *interface-type interface-number.subinterface-number* [**detail**] | *outer-id* [*interface-type interface-number* | **second-dot1q** [*inner-id* | **any**]] [**detail**]]

Syntax Description

internal	(Optional) Displays internal QinQ VLAN tag termination information. Used for troubleshooting purposes. The QinQ VLAN Tag Termination feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.
.*subinterface-number*	(Optional) Subinterface number in the range 1 to 4294967293. A period (**.**) must be entered between the *interface-number* argument and the *subinterface-number* argument.
detail	(Optional) Displays detailed information.
outer-id	(Optional) Outer VLAN identifier. The allowed range is from 1 to 4095.
second-dot1q	(Optional) Displays inner VLAN subinterface information.
inner-id	(Optional) Inner VLAN identifier. The allowed range is from 1 to 4095.
any	(Optional) Displays information for all the inner VLAN subinterfaces configured as "any." **Note** The **any** keyword is not supported on a subinterface configured for IPoQinQ because IP routing is not supported on ambiguous subinterfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(7)XI7	This command was integrated into Cisco IOS Release 12.3(7)XI7 and implemented on the Cisco 10000 series routers.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

If no arguments or keywords are entered, statistics for all of the 802.1Q VLAN IDs are displayed.

The **any** keyword is not supported for IPoQinQ because IP routing is not supported on ambiguous subinterfaces. However, the **second-dot1q** *inner-id* keyword and argument can be used on IPoQinQ for a specific inner VLAN ID that is not an ambiguous subinterface.

Note On the Cisco 10000 series router, the following is an implementation limitation—when a service policy is applied to a PPPoEoQinQ or IPoQinQ subinterface and the service policy drops some packets, the packets dropped are still displayed in the outgoing packet counters as output.

Note For the Cisco ASR 1000 Series Aggregation Services Router only, the command output includes the total number of packets dropped from the shared port adapter (SPA) because of ingress oversubscription on the VLAN. An example of the output is included in the "Cisco ASR 1000 Series Router: Example" section below.

Examples

802.1Q VLAN Statistics: Example

The output from the **show vlans dot1q** command displays the statistics for all the 802.1Q VLAN IDs. Only the outer VLAN IDs are displayed here.

```
Router# show vlans dot1q

Total statistics for 802.1Q VLAN 1:
   441 packets, 85825 bytes input
   1028 packets, 69082 bytes output
Total statistics for 802.1Q VLAN 101:
   5173 packets, 510384 bytes input
   3042 packets, 369567 bytes output
Total statistics for 802.1Q VLAN 201:
   1012 packets, 119254 bytes input
   1018 packets, 120393 bytes output
Total statistics for 802.1Q VLAN 301:
   3163 packets, 265272 bytes input
   1011 packets, 120750 bytes output
Total statistics for 802.1Q VLAN 401:
   1012 packets, 119254 bytes input
   1010 packets, 119108 bytes output
```

Table 36 describes the significant fields shown in the display.

Table 36 show vlans dot1q Field Descriptions

Field	Description
Total statistics for 802.1Q VLAN 1	Statistics are shown for the VLAN ID with the specified outer ID.
packets	Number of packets encapsulated by the 802.1Q QinQ VLAN.
bytes input	Number of bytes input.
bytes output	Number of bytes output.

The following sample output from the **show vlans dot1q** command displays the statistics for the 802.1Q VLAN subinterface configured on Gigabit Ethernet interface 5/0:

```
Router# show vlans dot1q GigabitEthernet 5/0.1011001

GigabitEthernet5/0.1011001 (101/1001)
   1005 packets, 122556 bytes input
   1023 packets, 125136 bytes output
```

Table 37 describes the significant fields shown in the display.

Table 37 show vlans dot1q (subinterface) Field Descriptions

Field	Description
GigabitEthernet5/0.1011001 (101/1001)	Statistics are shown for subinterface Gigabit Ethernet 5/0.1011001 with an outer VLAN ID of 101 and an inner VLAN ID of 1001.
packets	Number of packets encapsulated by the 802.1Q QinQ VLAN.
bytes input	Number of bytes input.
bytes output	Number of bytes output.

The following sample output from the **show vlans dot1q** command displays the summary statistics for all of the VLAN subinterfaces under the physical interface Gigabit Ethernet 5/0 that have an outer VLAN ID of 101:

```
Router# show vlans dot1q 101 GigabitEthernet 5/0

Total statistics for 802.1Q VLAN 101 on GigabitEthernet5/0:
   5218 packets, 513444 bytes input
   3042 packets, 369567 bytes output
```

The following sample output from the **show vlans dot1q** command displays the individual subinterface statistics and summary statistics for all the VLAN subinterfaces under the physical interface Gigabit Ethernet 5/0 that have an outer VLAN ID of 101:

```
Router# show vlans dot1q 101 GigabitEthernet 5/0 detail

GigabitEthernet5/0.101 (0)
   3220 packets, 269148 bytes input
   1008 packets, 119622 bytes output
GigabitEthernet5/0.1019999 (101/1-1000,1003-2000)
   0 packets, 0 bytes input
   3 packets, 1143 bytes output
GigabitEthernet5/0.1011001 (101/1001)
   1005 packets, 122556 bytes input
   1023 packets, 125136 bytes output
GigabitEthernet5/0.1011002 (101/1002)
   1005 packets, 122556 bytes input
   1008 packets, 123666 bytes output
Total statistics for 802.1Q VLAN 101 on GigabitEthernet5/0:
   5230 packets, 514260 bytes input
   3042 packets, 369567 bytes output
```

The following sample output from the **show vlans dot1q** command displays the statistics for an outer VLAN and inner VLAN ID combination. This is a summary that displays the total for all the subinterfaces on the router that are configured with the specified IDs.

Note When multiple inner VLANs are used, the statistics displayed are at subinterface-level granularity, not VLAN-ID granularity. For example, when a range of inner VLAN IDs is assigned to a subinterface, the statistics are reported only at the subinterface level. Statistics are not available for each inner VLAN ID.

```
Router# show vlans dot1q 101 second-dot1q 1001 detail

GigabitEthernet5/0.1011001 (101/1001)
   1005 packets, 122556 bytes input
   1023 packets, 125136 bytes output
Total statistics for Outer/Inner VLAN 101/1001:
   1005 packets, 122556 bytes input
   1023 packets, 125136 bytes output
```

The following sample output from the **show vlans dot1q** command displays the statistics for a specific outer VLAN ID of 301 and an inner VLAN ID of any. This is a summary that displays the total for all of the subinterfaces on the router that are configured with the specified IDs.

```
Router# show vlans dot1q 301 second-dot1q any

GigabitEthernet5/0.301999 (301/any)
   0 packets, 0 bytes input
   3 packets, 1128 bytes output
Total statistics for Outer/Inner VLAN 301/"any":
   0 packets, 0 bytes input
   3 packets, 1128 bytes output
```

QinQ Subsystem Information: Example

The following sample output from the **show vlans dot1q** command displays some internal information about the QinQ subsystem and is used for troubleshooting purposes (typically by Cisco engineers):

```
Router# show vlans dot1q internal

Internal VLAN representation on FastEthernet0/0:
VLAN Id: 1    (.1Q, Fa0/0)
VLAN Id: 201  (.1Q-in-.1Q tree, 3 elements)
  Inner VLAN Id: (0   -0   ) Fa0/0.201
  dot1q software subblock bitlist missing
  Inner VLAN Id: (2001-2001) Fa0/0.2012001
  2001
  Inner VLAN Id: (2002-2002) Fa0/0.2012002
  2002
  "any" Fa0/0.201999
VLAN Id: 401  (.1Q-in-.1Q tree, 3 elements)
  Inner VLAN Id: (0   -0   ) Fa0/0.401
  dot1q software subblock bitlist missing
  Inner VLAN Id: (100 -900 ) Fa0/0.4019999
  100-900,1001-2000
  Inner VLAN Id: (1001-2000) Fa0/0.4019999
  100-900,1001-2000
Internal VLAN representation on GigabitEthernet5/0:
VLAN Id: 1    (.1Q, Gi5/0)
VLAN Id: 101  (.1Q-in-.1Q tree, 5 elements)
  Inner VLAN Id: (0   -0   ) Gi5/0.101
  dot1q software subblock bitlist missing
  Inner VLAN Id: (1   -1000) Gi5/0.1019999
  1-1000,1003-2000
  Inner VLAN Id: (1001-1001) Gi5/0.1011001
  1001
  Inner VLAN Id: (1002-1002) Gi5/0.1011002
  1002
  Inner VLAN Id: (1003-2000) Gi5/0.1019999
  1-1000,1003-2000
VLAN Id: 301  (.1Q-in-.1Q tree, 1 elements)
  Inner VLAN Id: (0   -0   ) Gi5/0.301
  dot1q software subblock bitlist missing
  "any" Gi5/0.301999
```

Cisco ASR 1000 Series Router: Example

The following is an example of the output displayed on the Cisco ASR 1000 series router only. For the Cisco ASR 1000 series router only, the command output includes the total number of packets dropped from the SPA due to ingress over subscription on the VLAN.

```
Router# show vlans dot1q gigabitEthernet 0/0/3.1

GigabitEthernet0/0/3.1 (0)
   133279760 packets, 8529904640 bytes input
   0 packets, 0 bytes output
   121997683 oversub packet drops
```

Table 38 describes the significant fields shown in the display.

Table 38 show vlans dot1q (Cisco ASR 1000 Series Router) Field Descriptions

Field	Description
GigabitEthernet0/0/3.1	Statistics are shown for Gigabit Ethernet subinterface 0/0/3.1.
packets	Number of packets encapsulated by the 802.1Q QinQ VLAN.
bytes input	Number of bytes input.
bytes output	Number of bytes output.
oversub packet drops	Number of packets dropped from the SPA due to ingress over subscription on the VLAN.

Related Commands

Command	Description
encapsulation dot1q	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
vlan (VLAN)	Configures a specific VLAN.
vlan database	Enters VLAN configuration mode.

show vlans tokenring

To display Token Ring VLANs, use the **show vlans tokenring** command in user EXEC or privileged EXEC mode.

show vlans tokenring

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
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.
Cisco IOS XE Release 2.1	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to use the **show vlans tokenring** command. The fields shown in the display are self-explanatory.

```
Router# show vlans tokenring
```

When the **show vlans tokenring** command is executed on a device with the Token Ring configurations, the output consists of a list of Token Ring interfaces with VLAN configuration.

Related Commands

Command	Description
encapsulation dot1q	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
show vlans	Displays VLAN subinterfaces.
show vlans dot1q	Displays statistics about 802.1Q VLAN subinterfaces.

show vlan-switch

To display VLAN information, use the **show vlan-switch** command in user EXEC or privileged EXEC mode.

show vlan-switch [**brief** | **id** *vlan* | **internal usage** | **name** *name* | **summary**]

Syntax Description

brief	(Optional) Displays only a single line for each VLAN, identifying the VLAN, status, and ports.
id *vlan*	(Optional) Displays information about a single VLAN identified by VLAN ID number. The range is from 1 to 1005.
internal usage	(Optional) Displays VLAN internal usage information.
name *name*	(Optional) Displays information about a single VLAN identified by VLAN name. Valid values are ASCII strings from 1 to 32 characters.
summary	(Optional) Displays VLAN summary information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XT	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Each Ethernet switch port and Ethernet repeater group belongs to only one VLAN. Trunk ports can be on multiple VLANs.

Examples

The following is sample output from the example **show vlan-switch** command, which displays the VLAN parameters for all VLANs within the administrative domain:

```
Router# show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa4/0, Fa4/1, Fa4/2, Fa4/3
                                                Fa4/4, Fa4/5, Fa4/6, Fa4/7
                                                Fa4/8, Fa4/9, Fa4/10, Fa4/11
                                                Fa4/12, Fa4/13, Fa4/14, Fa4/15
                                                Fa4/16, Fa4/17, Fa4/18, Fa4/19
                                                Fa4/20, Fa4/21, Fa4/22, Fa4/23
                                                Fa4/24, Fa4/25, Fa4/26, Fa4/27
                                                Fa4/28, Fa4/29, Fa4/30, Fa4/31
                                                Fa4/32, Fa4/33, Fa4/34, Fa4/35
                                                Gi4/0, Gi4/1, Po1
2    VLAN0002                         active
3    VLAN0003                         active
5    VLAN0005                         active
1002 fddi-default                     active
```

```
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      0      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

Table 39 describes the significant fields shown in the display.

Table 39 show vlan Field Descriptions

Field	Description
VLAN	VLAN number.
Name	Name of the VLAN, if configured.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BridgeNo	Bridge number for the VLAN, if applicable.
Stp	Spanning-Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—Possible values are source-route bridging (SRB) and source-route transparent bridging (SRT); the default is SRB.
Trans1, Trans2	Types of translational bridges that the VLAN in the VLAN column is configured to translate to. Translational bridge VLANs must be a VLAN media type different from the affected VLAN; if two VLANs are specified, each one must be a different type. Common VLAN types include Ethernet (enet), FDDI (fdnet), and Token Ring (tnet). The numbers in the Trans1 and Trans2 columns refer to the VLAN ID numbers of the translational bridge VLANs. **Note** The term *VLAN translation* is also used in Cisco configuration guides for mapping specific VLANs in a given trunk to another VLAN that is of the same media type. In this context the term *VLAN translation* refers to a form of VLAN mapping that is using the term *VLAN translation* to describe it.

Related Commands

Command	Description
vlan (VLAN)	Configures specific VLANs.

show vtp

To display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters, use the **show vtp** command in privileged EXEC mode.

show vtp {**counters** | **interface** [*type*/*number*] | **status** | **password** | **devices** [**conflicts**]}

Syntax Description

counters	Displays the VTP counters for the switch.
interface	Displays information for all interfaces.
type/*number*	(Optional) A specific interface.
status	Displays general information about the VTP management domain.
password	Displays VTP password in VTP version 3 domain.
devices	Displays VTP version 3 domain information.
conflicts	(Optional) Displays only devices that have conflicting servers in a VTP version 3 domain.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2(8)SA4	This command was introduced.
12.2(2)XT	This command was implemented on the 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 the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command on the Supervisor Engine 2 was extended to Cisco IOS Release12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The **password**, **devices**, and **conflicts** keywords were added to support VTP version 3 on the Cisco 7600 series routers.
12.2(33)SXI	The output for counters and status were updated to include VTPv3 information.

Usage Guidelines

In the output of the **show vtp status** command, the last modified time is of the modifier itself. For example, the time displayed in the line “Configuration last modified by 7.0.22.11 at 5-5-06 05:51:49”, is the time that the modifier (7.0.22.11) last modified the VLAN configuration.

Examples

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

```
Router# show vtp counters

VTP statistics:
Summary advertisements received : 0
Subset advertisements received : 0
Request advertisements received : 0
Summary advertisements transmitted : 6970
Subset advertisements transmitted : 0
Request advertisements transmitted : 0
Number of config revision errors : 0
Number of config digest errors : 0
Number of V1 summary errors : 0
VTP pruning statistics:
Trunk             Join Transmitted Join Received    Summary advts received from
                                                    non-pruning-capable device
---------------- ---------------- ---------------- --------------------------
Gi1/11            0                0                0
Gi8/10            0                0                0
Gi8/15            0                0                0
Gi8/16            0                0                0
Fa3/1             0                0                0
Fa3/2             0                0                0
Router#
```

This example shows how to display only those lines in the **show vtp** output that contain the word Summary:

```
Router# show vtp counters | include Summary

Summary advertisements received    : 1
Summary advertisements transmitted : 32
Trunk            Join Transmitted Join Received    Summary advts received from
Router#
```

This example shows how to display general information about the VTP management domain:

```
Router# show vtp status

VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0012.44dc.b800
MD5 digest                      : 0x61 0x98 0xD0 0xAD 0xA4 0x8C 0x53 0x35
Configuration last modified by 10.10.0.0 at 8-7-06 06:56:27
Local updater ID is 10.10.0.0 on interface Lo0 (first layer3 interface found)

Feature VLAN:
--------------
VTP Mode                         : Server
Maximum VLANs supported locally  : 1005
Number if existing VLANs         : 53
Revision                         : 1
Router#
```

Table 40 describes the significant fields shown in the display.

Table 40 show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update time stamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this switch on its trunk ports. Subset advertisements contain all the VTP information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update time stamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this switch on its trunk ports. Subset advertisements contain all the VTP information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of config revision errors	Number of revision errors. Whenever you define a new VLAN, delete an existing VLAN, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments. Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the message digest algorithm 5 (MD5) values do not match. This error indicates that the VTP password in the two switches is different, or the switches have different configurations. These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.

Table 40 show vtp counters Field Descriptions (continued)

Field	Description
Number of config digest errors	Number of MD5 errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually indicates that the VTP passwords in the two switches are different. To solve this problem, make sure the VTP password on all switches is the same. These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of V1 summary errors	Number of version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP version 1 frame. These errors indicate that at least one neighboring switch is either running VTP version 1 or VTP version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
Trunk	Trunk port participating in VTP pruning.
Join Transmitted	Number of VTP pruning messages transmitted on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary advts received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

The following is sample output from the **show vtp status** command for VTP version 1 and VTP version 2:

```
Router# show vtp status

VTP Version                     : 3 (capable)
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 37
VTP Operating Mode              : Server
VTP Domain Name                 : [smartports]
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x26 0xEE 0x0D 0x84 0x73 0x0E 0x1B 0x69
Configuration last modified by 172.20.52.19 at 7-25-08 14:33:43
Local updater ID is 172.20.52.19 on interface Gi5/2 (first layer3 interface fou)
VTP version running             : 2
```

Table 41 describes the significant fields shown in the display.

Table 41 show vtp status Field Descriptions

Field	Description
VTP Version	**Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers** Displays the VTP version operating on the switch. By default, switches implement version 1. **Catalyst Switches** Displays the VTP version operating on the switch. By default, Catalyst 2900 and 3500 XL switches implement version 1 but can be set to version 2.
Configuration Revision	Current configuration revision number on this switch.
Maximum VLANs supported locally	Maximum number of VLANs supported locally.
Number of existing VLANs	Number of existing VLANs.

Table 41 show vtp status Field Descriptions (continued)

Field	Description
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. • Server—A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all VLAN information in the current VTP database from nonvolatile storage after reboot. By default, every switch is a VTP server. • Client—A switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not transmit VTP advertisements until it receives advertisements to initialize its VLAN database. • Transparent—A switch in VTP transparent mode is disabled for VTP, does not transmit advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. The configuration of multi-VLAN ports causes the switch to automatically enter transparent mode. • Off—When VTP is disabled using off mode, the switch behaves the same as in VTP transparent mode except that VTP advertisements are not forwarded. **Note** Catalyst 2912MF, 2924M, and 3500 XL switches support up to 250 VLANs. All other Catalyst 2900 XL switches support up to 64 VLANs. For Catalyst 2912MF, 2924M, and 3500 XL switches, if you define more than 250 VLANs or if the switch receives an advertisement that contains more than 250 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that sent it into transparent mode. For all other Catalyst 2900 XL switches, if you define more than 64 VLANs or if the switch receives an advertisement that contains more than 64 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that sent it into transparent mode.
VTP Domain Name	Name that identifies the administrative domain for the switch.

Table 41 show vtp status Field Descriptions (continued)

Field	Description
VTP Pruning Mode	**Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers** VTP pruning mode is not supported on the Cisco 2600, Cisco 3600, and 3700 series routers. **Catalyst Switches, Cisco 7600 Series Routers** Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP V2 Mode	Displays if VTP version 2 mode is enabled. All VTP version 2 switches operate in version 1 mode by default. Each VTP switch automatically detects the capabilities of all other VTP devices. A network of VTP devices should be configured to version 2 only if all VTP switches in the network can operate in version 2 mode.
VTP Traps Generation	Displays whether VTP traps are transmitted to a network management station.
MD5 digest	16-byte checksum of the VTP configuration.
Configuration last modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

The following is sample output from the **show vtp status** command for all three VTP versions on the Cisco 7600 series routers running Release 12.2(33)SRC and later.

This example shows how to verify the configuration when the device is running VTP version 1:

```
Router# show vtp status

VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : Lab_Network
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : 0016.9c6d.5300
Configuration last modified by 127.0.0.12 at 10-18-07 10:12:42
Local updater ID is 127.00.12 at 10-18-07 10:2:42

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum number of existing VLANs : 5
Configuration Revision          : 1
MD5 digest                      : 0x92 0xF1 0xE8 0x52 0x2E ox5C 0x36 0x10 0x70 0x61 0xB8
                                0x24 0xB6 0x93 0x21 0x09
Router#
```

This example shows how to verify the configuration when the device is running VTP version 2:

```
Router# show vtp status

VTP Version capable          : 1 to 3
```

```
VTP version running          : 2
VTP Domain Name              : Lab_Network
VTP Pruning Mode             : Disabled
VTP Traps Generation         : Disabled
Device ID                    : 0012.44dc.b800
Configuration lst modified by 127.0.0.12 at 10-18-07 10:38:45
Local updater ID is 127.0.0.12 on interface EO 0/0 (first interface found)

Feature VLAN:
--------------
VTP Operating Mode           : Server
Maximum VLANs supported locally: 1005
Number of existing VLANs     : 1005
Configuration Revision       : 1
MD5 digest                   : 0x2E 0x6B 0x99 0x58 0xA2 0x4F 0xD5 0x150x70 0x61 0xB8
                             0x24 0xB6 0x93 0x21 0x09
Router#
```

This example shows how to verify the configuration when the device is running VTP version 3:

```
Router# show vtp status

VTP Version capable          : 1 to 3
VTP version running          : 3
VTP Domain Name              : Lab_Network
VTP Pruning Mode             : Disabled
VTP Traps Generation         : Disabled
Device ID                    : 0012.44dc.b800

Feature VLAN:
--------------
VTP Operating Mode              : Server
Number of existing VLANs        : 1005
Number of existing extended VLANs: 3074
Configuration Revision          : 18
Primary ID                      : 0012.4371.9ec0
Primary Description             :
Router#
```

Table 42 describes the significant fields shown in the displays.

Table 42 show vtp status Field Descriptions (Cisco 7600 Series Routers Release 12.2(33)SRC and Later)

Field	Description
VTP Version capable	Versions of VTP that the device is capable of running.
VTP Version running	Version of VTP that the device is running.
VTP Domain Name	Name that identifies the administrative domain for the device.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk lines that the traffic must use to access the appropriate network devices.
VTP Traps Generation	Displays whether VTP traps are transmitted to a network management station.
Device ID	MAC address of the local device.

Table 42 show vtp status Field Descriptions (Cisco 7600 Series Routers Release 12.2(33)SRC and Later) (continued)

Field	Description
Configuration last modified Configuration lst modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.
VTP Operating Mode	VTP Mode (Client, Server, Transparent, Off) listed by feature type.
Maximum VLANs supported locally	Maximum number of VLANs supported locally.
Maximum number of existing VLANs	Number of existing VLANs.
Number of existing extended VLANs	Number of existing extended VLANs.
Configuration Revision	Configuration revision number for the specific feature.
Primary ID	MAC address of primary server.
Primary Description	Name of primary server.
MD5 digest	32-bit checksum of the VTP configuration.

This example shows how to display information for a specific interface:

```
Router# show vtp interface GigabitEthernet2/4

Interface              VTP Status
-------------------------------------
GigabitEthernet2/4     enabled
```

This example shows how a password is displayed when it is configured using the **hidden** keyword (VTP version 3 only):

```
Router# show vtp password

VTP Password: 89914640C8D90868B6A0D8103847A733
Router#
```

This example shows how to display information about all VTP devices in the domain:

```
Router# show vtp devices

Gathering information from the domain, please wait.
VTP Database Conf switch ID      Primary Server Revision  System Name
             lict
------------ ---- -------------- ----------------------- ------------------
VLAN         Yes  00b0.8e50.d000 000c.0412.6300 12354     main.cisco.com
MST          No   00b0.8e50.d000 0004.AB45.6000 24        main.cisco.com
VLAN         Yes  000c.0412.6300=000c.0412.6300 67        querty.cisco.com
```

Table 43 describes the significant fields shown in the display.

Table 43 show vtp devices Field Descriptions

Field	Description
VTP Database	Displays the feature (database) type (VLAN or MST) of each server.
Conflict	Yes is displayed in this column if the server is in conflict with the local server for the feature. A conflict is detected when two devices in the same domain do not have the same primary server for the given database.
Switch ID	The MAC address of the server.
Primary Server	The MAC address of the primary server for the device identified in the Switch ID column. If a device is configured with a database that it originated, and equal sign (=) appears between the Primary Server field and the Switch ID field.
Revision	Revision number of the VTP database.
System Name	String provided to more easily identify the system.

Related Commands

Command	Description
clear vtp counters	Clears the VTP and pruning counters.
vtp	Configures the VTP mode.

shutdown vlan

To shut down local traffic on a specified VLAN, use the **shutdown vlan** command in global configuration mode. To restart local traffic on the VLAN, use the **no** form of this command.

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

Syntax Description

vlan-id	VLAN number of the VLAN to be locally shut down; valid values are from 2 to 1001.

Command Default

Local traffic on a specified VLAN is not shut down.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command does not support extended-range VLANs.

Examples

This example shows how to shut down traffic on VLAN 2:

```
Router(config)# shutdown vlan 2
```

snmp trap mac-notification change

To enable the Simple Network Management Protocol (SNMP) trap notification on a LAN port when MAC addresses are added to or removed from the address table, use the **snmp trap mac-notification change** command in interface configuration mode. To disable the SNMP trap notification on a LAN port when MAC addresses are added to or removed from the address table, use the **no** form of this command.

snmp trap mac-notification change [**added** | **removed**]

no snmp trap mac-notification change

Syntax Description

added	(Optional) Sends notification only when a MAC address is added to the table.
removed	(Optional) Sends notification only when a MAC address is removed to the table.

Command Default

The SNMP trap notification is disabled.

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example shows how to enable the SNMP trap notification on a LAN port when MAC addresses are added to the address table:

```
Router(config-if)# snmp trap mac-notification change added
```

The following example shows how to enable the SNMP trap notification on a LAN port when MAC addresses are removed from the address table:

```
Router(config-if)# snmp trap mac-notification change removed
```

The following example shows how to disable the SNMP trap notification on a LAN port:

```
Router(config-if)# no snmp trap mac-notification change
```

Related Commands

Command	Description
mac-address-table notification change	Sends a notification of the dynamic changes to the MAC address table.

spanning-tree backbonefast

To enable BackboneFast to allow a blocked port on a switch to change immediately to a listening mode, use the **spanning-tree backbonefast** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree backbonefast

no spanning-tree backbonefast

Syntax Description

This command has no arguments or keywords.

Command Default

BackboneFast is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(15)ZJ	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
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(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

BackboneFast should be enabled on all of the Cisco routers containing an Ethernet switch network module. BackboneFast provides for fast convergence in the network backbone after a spanning-tree topology change. It enables the switch to detect an indirect link failure and to start the spanning-tree reconfiguration sooner than it would under normal spanning-tree rules.

Use the **show spanning-tree** privileged EXEC command to verify your settings.

Examples

The following example shows how to enable BackboneFast on the switch:

```
Router(config)# spanning-tree backbonefast
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree bpdufilter

To enable bridge protocol data unit (BPDU) filtering on the interface, use the **spanning-tree bpdufilter** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree bpdufilter {**enable** | **disable**}

no spanning-tree bpdufilter

Syntax Description

enable	Enables BPDU filtering on this interface.
disable	Disables BPDU filtering on this interface.

Command Default

The setting that is already configured when you enter the **spanning-tree portfast bpdufilter default** command.

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(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.

Usage Guidelines

Caution Be careful when you enter the **spanning-tree bpdufilter enable** command. Enabling BPDU filtering on an interface is similar to disabling the spanning tree for this interface. If you do not use this command correctly, you might create bridging loops.

Entering the **spanning-tree bpdufilter enable** command to enable BPDU filtering overrides the PortFast configuration.

When configuring Layer 2-protocol tunneling on all the service-provider edge switches, you must enable spanning-tree BPDU filtering on the 802.1Q tunnel ports by entering the **spanning-tree bpdufilter enable** command.

BPDU filtering prevents a port from sending and receiving BPDUs. The configuration is applicable to the whole interface, whether it is trunking or not. This command has three states:

- **spanning-tree bpdufilter enable**—Unconditionally enables BPDU filtering on the interface.
- **spanning-tree bpdufilter disable**—Unconditionally disables BPDU filtering on the interface.
- **no spanning-tree bpdufilter**—Enables BPDU filtering on the interface if the interface is in operational PortFast state and if you configure the **spanning-tree portfast bpdufilter default** command.

Use the **spanning-tree portfast bpdufilter default** command to enable BPDU filtering on all ports that are already configured for PortFast.

Examples

This example shows how to enable BPDU filtering on this interface:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast bpdufilter default	Enables BPDU filtering by default on all PortFast ports.

spanning-tree bpduguard

To enable bridge protocol data unit (BPDU) guard on the interface, use the **spanning-tree bpduguard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree bpduguard {**enable** | **disable**}

no spanning-tree bpduguard

Syntax Description

enable	Enables BPDU guard on this interface.
disable	Disables BPDU guard on this interface.

Command Default

The setting that is already configured when you enter the **spanning-tree portfast bpduguard default** command.

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(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.

Usage Guidelines

BPDU guard prevents a port from receiving BPDUs. Typically, this feature is used in a service-provider environment where the network administrator wants to prevent an access port from participating in the spanning tree. If the port still receives a BPDU, it is put in the error-disabled state as a protective measure. This command has three states:

- **spanning-tree bpduguard enable**—Unconditionally enables BPDU guard on the interface.
- **spanning-tree bpduguard disable**—Unconditionally disables BPDU guard on the interface.
- **no spanning-tree bpduguard**—Enables BPDU guard on the interface if it is in the operational PortFast state and if the **spanning-tree portfast bpduguard default** command is configured.

Examples

This example shows how to enable BPDU guard on this interface:

```
Router(config-if)# spanning-tree bpduguard enable
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast bpduguard default	Enables BPDU guard by default on all PortFast ports.

spanning-tree bridge assurance

To enable Bridge Assurance on all network ports on the switch, use the **spanning-tree bridge assurance** command in global configuration mode. To disable Bridge Assurance, use the **no** form of this command.

spanning-tree bridge assurance

no spanning-tree bridge assurance

Syntax Description

This command has no arguments or keywords.

Command Default

Bridge Assurance is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

Bridge Assurance protects against a unidirectional link failure or other software failure and a device that continues to forward data traffic when it is no longer running the spanning tree algorithm.

Bridge Assurance is enabled only on spanning tree network ports that are point-to-point links. Both ends of the link must have Bridge Assurance enabled. If the device on one side of the link has Bridge Assurance enabled and the device on the other side either does not support Bridge Assurance or does not have this feature enabled, the connecting port is blocked.

Disabling Bridge Assurance causes all configured network ports to behave as normal spanning tree ports.

Examples

This example shows how to enable Bridge Assurance on all network ports on the switch:

```
Router(config)# spanning-tree bridge assurance
Router(config)#
```

This example shows how to disable Bridge Assurance on all network ports on the switch:

```
Router(config)# no spanning-tree bridge assurance
Router(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree cost

To set the path cost of the interface for Spanning Tree Protocol (STP) calculations, use the **spanning-tree cost** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

spanning-tree cost *cost*

no spanning-tree cost

Syntax Description

cost	Path cost; valid values are from 1 to 200000000 for Cisco IOS Releases 12.1(3a)E and later releases and from 1 to 65535 for Cisco IOS releases prior to Cisco IOS Release 12.1(3a)E.

Command Default

The default path cost is computed from the bandwidth setting of the interface; default path costs are:

Ethernet: 100
16-Mb Token Ring: 62
FDDI: 10
FastEthernet: 10
ATM 155: 6
GigibitEthernet: 1
HSSI: 647

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
12.1(3a)E	This command was modified to support 32-bit path cost.
12.2(2)XT	This command was introduced on the 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 the 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.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you specify a value for the cost argument, higher values indicate higher costs. This range applies regardless of the protocol type specified.

Examples

The following example shows how to access an interface and set a path cost value of 250 for the spanning tree VLAN associated with that interface:

```
Router(config)# interface ethernet 2/0
Router(config-if)# spanning-tree cost 250
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning-tree port-priority	Sets an interface priority when two bridges tie for position as the root bridge.
spanning-tree portfast (global)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree portfast (interface)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree uplinkfast	Enables the UplinkFast feature.
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree etherchannel guard misconfig

To display an error message when a loop due to a channel misconfiguration is detected, use the **spanning-tree etherchannel guard misconfig** command in global configuration mode. To disable the error message, use the **no** form of this command.

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

Syntax Description

This command has no arguments or keywords.

Command Default

Error messages are displayed.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

EtherChannel uses either Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP) and does not work if the EtherChannel mode of the interface is enabled using the **channel-group** *group-number* **mode on** command.

The **spanning-tree etherchannel guard misconfig** command detects two types of errors: misconfiguration and misconnection errors. A misconfiguration error is an error between the port-channel and an individual port. A misconnection error is an error between a switch that is channeling more ports and a switch that is not using enough Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) to detect the error. In this case, the switch will only error disable an EtherChannel if the switch is a nonroot switch.

When an EtherChannel-guard misconfiguration is detected, this error message displays:

```
msgdef(CHNL_MISCFG, SPANTREE, LOG_CRIT, 0, "Detected loop due to etherchannel
misconfiguration of %s %s")
```

To determine which local ports are involved in the misconfiguration, enter the **show interfaces status err-disabled** command. To check the EtherChannel configuration on the remote device, enter the **show etherchannel summary** command on the remote device.

After you correct the configuration, enter the **shutdown** and the **no shutdown** commands on the associated port-channel interface.

Examples

This example shows how to enable the EtherChannel-guard misconfiguration:

```
Router(config)# spanning-tree etherchannel guard misconfig
Router(config)#
```

Related Commands

Command	Description
show etherchannel summary	Displays the EtherChannel information for a channel.
show interfaces status err-disabled	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
shutdown	Disables an interface.

spanning-tree extend system-id

To enable the extended-system ID feature on chassis that support 1024 MAC addresses, use the **spanning-tree extend system-id** command in global configuration mode. To disable the extended system identification, use the **no** form of this command.

spanning-tree extend system-id

no spanning-tree extend system-id

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled on systems that do not provide 1024 MAC addresses.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The Catalyst 6500 series switch can support 64 or up to 1024 MAC addresses. For a Catalyst 6500 series switch with 64 MAC addresses, STP uses the extended-system ID and a MAC address to make the bridge ID unique for each VLAN.

You cannot disable the extended-system ID on a Catalyst 6500 series switch that supports 64 MAC addresses.

Enabling or disabling the extended-system ID updates the bridge IDs of all active Spanning Tree Protocol (STP) instances, which might change the spanning-tree topology.

Examples

This example shows how to enable the extended-system ID:

```
Router(config)# spanning-tree extend system-id
Router(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree guard

To enable or disable the guard mode, use the **spanning-tree guard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree guard {**loop** | **root** | **none**}

no spanning-tree guard

Syntax Description

loop	Enables the loop-guard mode on the interface.
root	Enables root-guard mode on the interface.
none	Sets the guard mode to none.

Command Default

Guard mode is disabled.

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(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.

Examples

This example shows how to enable root guard:

```
Router(config-if)# spanning-tree guard root
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree loopguard default	Enables loop guard as a default on all ports of a given bridge.

spanning-tree link-type

To configure a link type for a port, use the **spanning-tree link-type** command in the interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree link-type

Syntax Description

point-to-point	Specifies that the interface is a point-to-point link.
shared	Specifies that the interface is a shared medium.

Command Default

Link type is automatically derived from the duplex setting unless you explicitly configure the link type.

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(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.

Usage Guidelines

Rapid Spanning Tree Protocol Plus (RSTP+) fast transition works only on point-to-point links between two bridges.

By default, the switch derives the link type of a port from the duplex mode. A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link.

If you designate a port as a shared link, RSTP+ fast transition is forbidden, regardless of the duplex setting.

Examples

This example shows how to configure the port as a shared link:

```
Router(config-if)# spanning-tree link-type shared
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree interface	Displays information about the spanning-tree state.

spanning-tree loopguard default

To enable loop guard as a default on all ports of a given bridge, use the **spanning-tree loopguard default** command in global configuration mode. To disable loop guard, use the **no** form of this command.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description

This command has no arguments or keywords.

Command Default

Loop guard is disabled.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Loop guard provides additional security in the bridge network. Loop guard prevents alternate or root ports from becoming the designated port due to a failure that could lead to a unidirectional link.

Loop guard operates only on ports that are considered point to point by the spanning tree.

The individual loop-guard port configuration overrides this command.

Examples

This example shows how to enable loop guard:

```
Router(config)# spanning-tree loopguard default
Router(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree guard	Enables or disables the guard mode.

spanning-tree mode

To switch between Per-VLAN Spanning Tree+ (PVST+), Rapid-PVST+, and Multiple Spanning Tree (MST) modes, use the **spanning-tree mode** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mode [**pvst** | **mst** | **rapid-pvst**]

no spanning-tree mode

Syntax Description

pvst	(Optional) PVST+ mode.
mst	(Optional) MST mode.
rapid-pvst	(Optional) Rapid-PVST+ mode.

Command Default

pvst

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Caution Be careful when using the **spanning-tree mode** command to switch between PVST+, Rapid-PVST+, and MST modes. When you enter the command, all spanning-tree instances are stopped for the previous mode and are restarted in the new mode. Using this command may cause disruption of user traffic.

Examples

This example shows how to switch to MST mode:

```
Router(config)# spanning-tree mode mst
Router(config)#
```

This example shows how to return to the default mode (PVST+):

```
Router(config)# no spanning-tree mode
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst

To set the path cost and port-priority parameters for any Multiple Spanning Tree (MST) instance (including the Common and Internal Spanning Tree [CIST] with instance ID 0), use the **spanning-tree mst** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance-id* {{**cost** *cost* | **port-priority** *priority*} | **pre-standard**}

no spanning-tree mst *instance-id* {{**cost** | **port-priority**} | **pre-standard**}

Syntax Description

instance-id	Instance ID number; valid values are from 0 to 15.
cost *cost*	Path cost for an instance; valid values are from 1 to 200000000.
port-priority *priority*	Port priority for an instance; valid values are from 0 to 240 in increments of 16.
pre-standard	Configures prestandard MST BPDU transmission on the interface.

Command Default

The defaults are as follows:

- *cost* depends on the port speed; the faster interface speeds indicate smaller costs. MST always uses long path costs.
- *priority* is **128**.

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(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.

Usage Guidelines

Higher **cost** *cost* values indicate higher costs. When entering the *cost*, do not include a comma in the entry; for example, enter **1000**, not **1,000**.

Higher **port-priority** *priority* values indicate smaller priorities.

Examples

This example shows how to set the interface path cost:

```
Router(config-if)# spanning-tree mst 0 cost 17031970
Router(config-if)#
```

This example shows how to set the interface priority:

```
Router(config-if)# spanning-tree mst 0 port-priority 64
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree port-priority	Sets an interface priority when two bridges vie for position as the root bridge.

spanning-tree mst configuration

To enter MST-configuration submode, use the **spanning-tree mst configuration** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description

This command has no arguments or keywords.

Command Default

The default value for the Multiple Spanning Tree (MST) configuration is the default value for all its parameters:

- No VLANs are mapped to any MST instance (all VLANs are mapped to the Common and Internal Spanning Tree [CIST] instance).
- The region name is an empty string.
- The revision number is 0.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The MST configuration consists of three main parameters:

- Instance VLAN mapping—See the **instance** command
- Region name—See the **name (MST configuration submode)** command
- Configuration revision number—See the **revision** command

The **abort** and **exit** commands allow you to exit MST configuration submode. The difference between the two commands depends on whether you want to save your changes or not.

The **exit** command commits all the changes before leaving MST configuration submode. If you do not map secondary VLANs to the same instance as the associated primary VLAN, when you exit MST-configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

The **abort** command leaves MST-configuration submode without committing any changes.

Changing an MST-configuration submode parameter can cause connectivity loss. To reduce service disruptions, when you enter MST-configuration submode, make changes to a copy of the current MST configuration. When you are done editing the configuration, you can apply all the changes at once by using the **exit** keyword, or you can exit the submode without committing any change to the configuration by using the **abort** keyword.

In the unlikely event that two users commit a new configuration at exactly at the same time, this warning message displays:

```
% MST CFG:Configuration change lost because of concurrent access
```

Examples

This example shows how to enter MST-configuration submode:

```
Router(config)# spanning-tree mst configuration
Router(config-mst)#
```

This example shows how to reset the MST configuration to the default settings:

```
Router(config)# no spanning-tree mst configuration
Router(config)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST)	Sets the name of an MST region.
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 forward-time

To set the forward-delay timer for all the instances on the Catalyst 6500 series switch, use the **spanning-tree mst forward-time** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description

seconds	Number of seconds to set the forward-delay timer for all the instances on the Catalyst 6500 series switch; valid values are from 4 to 30 seconds.

Command Default

seconds is **15**.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to set the forward-delay timer:

```
Router(config)# spanning-tree mst forward-time 20
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst hello-time

To set the hello-time delay timer for all the instances on the Catalyst 6500 series switch, use the **spanning-tree mst hello-time** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description

seconds	Number of seconds to set the hello-time delay timer for all the instances on the Catalyst 6500 series switch; valid values are from 1 to 10 seconds.

Command Default

2 seconds

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you do not specify the *hello-time* value, the value is calculated from the network diameter.

Examples

This example shows how to set the hello-time delay timer:

```
Router(config)# spanning-tree mst hello-time 3
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst max-age

To set the max-age timer for all the instances on the Catalyst 6500 series switch, use the **spanning-tree mst max-age** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description

seconds	Number of seconds to set the max-age timer for all the instances on the Catalyst 6500 series switch; valid values are from 6 to 40 seconds.

Command Default

20 seconds

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to set the max-age timer:

```
Router(config)# spanning-tree mst max-age 40
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst max-hops

To specify the number of possible hops in the region before a bridge protocol data unit (BPDU) is discarded, use the **spanning-tree mst max-hops** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-hops *hopnumber*

no spanning-tree mst max-hops

Syntax Description

hopnumber	Number of possible hops in the region before a BPDU is discarded; valid values are from 1 to 255 hops.

Command Default

20 hops

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 Release 12.2(17d)SXB.
12.2(18)SXF	This command was changed to increase the maximum number of possible hops from 40 to 255 hops.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to set the number of possible hops:

```
Router(config)# spanning-tree mst max-hops 25
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst pre-standard

To configure a port to transmit only prestandard bridge protocol data units (BPDUs), use the **spanning-tree mst pre-standard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst pre-standard

no spanning-tree mst pre-standard

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to automatically detect prestandard neighbors.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXF	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

Even with the default configuration, the port can receive both prestandard and standard BPDUs.

Prestandard BPDUs are based on the Cisco IOS Multiple Spanning Tree (MST) implementation that was created before the IEEE standard was finalized. Standard BPDUs are based on the finalized IEEE standard.

If you configure a port to transmit prestandard BPDUs only, the prestandard flag displays in the **show spanning-tree** commands. The variations of the prestandard flag are as follows:

- Pre-STD (or pre-standard in long format)—This flag displays if the port is configured to transmit prestandard BPDUs and if a prestandard neighbor bridge has been detected on this interface.
- Pre-STD-Cf (or pre-standard (config) in long format)—This flag displays if the port is configured to transmit prestandard BPDUs but a prestandard BPDU has not been received on the port, the autodetection mechanism has failed, or a misconfiguration, if there is no prestandard neighbor, has occurred.
- Pre-STD-Rx (or pre-standard (rcvd) in long format)—This flag displays when a prestandard BPDU has been received on the port but it has not been configured to send prestandard BPDUs. The port will send prestandard BPDUs, but we recommend that you change the port configuration so that the interaction with the prestandard neighbor does not rely only on the autodetection mechanism.

If the MST configuration is not compatible with the prestandard (if it includes an instance ID greater than 15), only standard MST BPDUs are transmitted, regardless of the STP configuration on the port.

Examples

This example shows how to configure a port to transmit only prestandard BPDUs:

```
Router(config-if)# spanning-tree mst pre-standard
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst priority

To set the bridge priority for an instance, use the **spanning-tree mst priority** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance* **priority** *priority*

no spanning-tree mst priority

Syntax Description

instance	Instance identification number; valid values are from 0 to 4094.
priority *priority*	Specifies the bridge priority; see the "Usage Guidelines" section for valid values and additional information.

Command Default

priority is **32768**.

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 Release 12.2(17d)SXB.

Usage Guidelines

You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are **0**, **4096**, **8192**, **12288**, **16384**, **20480**, **24576**, **28672**, **32768**, **36864**, **40960**, **45056**, **49152**, **53248**, **57344**, and **61440**.

You can set the *priority* to **0** to make the switch root.

You can enter *instance* as a single instance or a range of instances, for example, 0-3,5,7-9.

Examples

This example shows how to set the bridge priority:

```
Router(config)# spanning-tree mst 0 priority 4096
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst root

To designate the primary and secondary root switch and set the timer value for an instance, use the **spanning-tree mst root** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance* **root** {**primary** | **secondary**} [**diameter** *diameter* [**hello-time** *seconds*]]

no spanning-tree mst *instance* **root**

Syntax Description

instance	Instance identification number; valid values are from 0 to 4094.
primary	Specifies the high enough priority (low value) to make the root of the spanning-tree instance.
secondary	Specifies the switch as a secondary root, should the primary root fail.
diameter *diameter*	(Optional) Specifies the timer values for the root switch that are based on the network diameter; valid values are from 1 to 7.
hello-time *seconds*	(Optional) Specifies the duration between the generation of configuration messages by the root switch.

Command Default

The **spanning-tree mst root** command has no default settings.

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 Release 12.2(17d)SXB.

Usage Guidelines

You can enter *instance* as a single instance or a range of instances, for example, 0-3,5,7-9.

The **spanning-tree mst root secondary** value is 16384.

The **diameter** *diameter* and **hello-time** *seconds* keywords and arguments are available for instance 0 only.

If you do not specify the *seconds* argument, the value for it is calculated from the network diameter.

Examples

This example shows how to designate the primary root switch and timer values for an instance:

```
Router(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
Router(config)# spanning-tree mst 5 root primary
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst simulate pvst (interface)

To override the global Per-VLAN Spanning Tree (PVST) simulation setting for a port, use the **spanning-tree mst simulate pvst** interface command in interface configuration mode. To return to the default PVST simulation setting, use the **no** form of this command.

spanning-tree mst simulate pvst [**disable**]

no spanning-tree mst simulate pvst

Syntax Description

disable	Disables PVST simulation on the interface.

Command Default

PVST simulation is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

PVST simulation is enabled by default so that an interface can interoperate between Multiple Spanning Tree (MST) and Rapid Per-VLAN Spanning Tree Plus (PVST+). To prevent an accidental connection to a device that does not run MST as the default Spanning Tree Protocol (STP) mode, you can disable PVST simulation. If you disable PVST simulation, the MST-enabled port moves to the blocking state once it detects it is connected to a Rapid PVST+-enabled port. This port remains in the inconsistent state until the port stops receiving Bridge Protocol Data Units (BPDUs), and then the port resumes the normal STP transition process.

Examples

This example shows how to prevent a port from automatically interoperating with a connecting device that is running Rapid PVST+:

```
Router(config)# interface gi3/13
Router(config-if)# spanning-tree mst simulate pvst disable
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree port-priority	Sets an interface priority when two bridges vie for position as the root bridge.

spanning-tree mst simulate pvst global

To enable Per-VLAN Spanning Tree (PVST) simulation globally, enter the **spanning-tree mst simulate pvst global** command in global configuration mode. To disable PVST simulation globally, enter the **no** form of this command.

spanning-tree mst simulate pvst global

no spanning-tree mst simulate pvst global

Syntax Description

This command has no arguments or keywords.

Command Default

PVST simulation is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

PVST simulation is enabled by default so that all interfaces on the device interoperate between Multiple Spanning Tree (MST) and Rapid Per-VLAN Spanning Tree Plus (PVST+). To prevent an accidental connection to a device that does not run MST as the default Spanning Tree Protocol (STP) mode, you can disable PVST simulation. If you disable PVST simulation, the MST-enabled port moves to the blocking state once it detects it is connected to a Rapid PVST+-enabled port. This port remains in the inconsistent state until the port stops receiving Bridge Protocol Data Units (BPDUs), and then the port resumes the normal STP transition process.

To override the global PVST simulation setting for a port, enter the **spanning-tree mst simulate pvst** interface command in the interface command mode.

Examples

This example shows how to prevent the switch from automatically interoperating with a connecting device that is running Rapid PVST+:

```
Router(config)# no spanning-tree mst simulate pvst global
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree mst simulate pvst (interface)	Overrides the global PVST simulation setting for a port.

spanning-tree pathcost method

To set the default path-cost calculation method, use the **spanning-tree pathcost method** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

Syntax Description

long	Specifies the 32-bit based values for default port-path costs.
short	Specifies the 16-bit based values for default port-path costs.

Command Default

short

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command applies to all the spanning-tree instances on the Catalyst 6500 series switch.

The **long** path-cost calculation method utilizes all 32 bits for path-cost calculation and yields values in the range of 1 through 200,000,000.

The **short** path-cost calculation method (16 bits) yields values in the range of 1 through 65535.

Examples

This example shows how to set the default path-cost calculation method to long:

```
Router(config#) spanning-tree pathcost method long
Router(config#)
```

This example shows how to set the default path-cost calculation method to short:

```
Router(config#) spanning-tree pathcost method short
Router(config#)
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree portfast (interface)

To enable PortFast mode where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire, use the **spanning-tree portfast** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast

spanning-tree portfast {**disable** | **edge** [**trunk**] | **network** | **trunk**}

no spanning-tree portfast

Syntax Description

disable	Disables PortFast on the interface.
edge	Enables PortFast edge mode on the interface.
network	Enables PortFast network mode on the interface.
trunk	Enables PortFast on the interface even in the trunk mode.

Command Default

The settings that are configured by the **spanning-tree portfast default** command.

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(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)SXI	Added **edge** [**trunk**] and **network** keywords.

Usage Guidelines

You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the Catalyst 6500 series switch and network operation.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

Be careful when using the **no spanning-tree portfast** command. This command does not disable PortFast if the **spanning-tree portfast default** command is enabled.

This command has these states:

- **spanning-tree portfast**—This command enables PortFast unconditionally on the given port.
- **spanning-tree portfast disable**—This command explicitly disables PortFast for the given port. The configuration line shows up in the running configuration because it is not the default.
- **spanning-tree portfast edge**—This command allows you to configure PortFast edge mode on the given port.

- **spanning-tree portfast network**—This command allows you to configure PortFast network mode on the given port.
- **spanning-tree portfast** [**edge**] **trunk**—This command allows you to configure PortFast on trunk ports. The **edge** keyword is required with **trunk** in Cisco IOS Release 12.2(33)SXI and later releases.

Note If you enter the **spanning-tree portfast trunk** command, the port is configured for PortFast even in the access mode.

- **no spanning-tree portfast**—This command implicitly enables PortFast if you define the **spanning-tree portfast default** command in global configuration mode and if the port is not a trunk port. If you do not configure PortFast globally, the **no spanning-tree portfast** command is equivalent to the **spanning-tree portfast disable** command.

Examples

This example shows how to enable PortFast mode in releases earlier than Cisco IOS Release 12.2(33)SXI:

```
Router(config-if)# spanning-tree portfast
Router(config-if)#
```

This example shows how to enable PortFast edge mode in Cisco IOS Release 12.2(33)SXI and later releases:

```
Router(config-if)# spanning-tree portfast edge
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast default	Enables PortFast by default on all access ports.

spanning-tree portfast bpdufilter default

To enable bridge protocol data unit (BPDU) filtering by default on all PortFast ports, use the **spanning-tree portfast bpdufilter default** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **spanning-tree portfast bpdufilter** command enables BPDU filtering globally on PortFast ports. BPDU filtering prevents a port from sending or receiving any BPDUs.

You can override the effects of the **portfast bpdufilter default** command by configuring BPDU filtering at the interface level.

Note Be careful when enabling BPDU filtering. The feature's functionality is different when you enable it on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled.

When enabled locally on a port, BPDU filtering prevents the Catalyst 6500 series switch from receiving or sending BPDUs on this port.

Caution Be careful when using this command. Using this command incorrectly can cause bridging loops.

Examples

This example shows how to enable BPDU filtering by default:

```
Router(config)# spanning-tree portfast bpdufilter default
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree bpdufilter	Enables BPDU filtering on the interface.

spanning-tree portfast bpduguard default

To enable bridge protocol data unit (BPDU) guard by default on all PortFast ports, use the **spanning-tree portfast bpduguard default** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Caution Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the Catalyst 6500 series switch and network operation.

BPDU guard disables a port if it receives a BPDU. BPDU guard is applied only on ports that are PortFast enabled and are in an operational PortFast state.

Examples

This example shows how to enable BPDU guard by default:

```
Router(config)# spanning-tree portfast bpduguard default
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree bpdufilter	Enables BPDU filtering on the interface.

spanning-tree portfast default

To enable PortFast by default on all access ports, use the **spanning-tree portfast default** command in global configuration mode. To disable PortFast by default on all access ports, use the **no** form of this command.

spanning-tree portfast {**edge** [**bpdufilter** | **bpduguard**] | **network** | **normal**} **default**

no spanning-tree portfast {**edge** [**bpdufilter** | **bpduguard**] | **network** | **normal**} **default**

Syntax Description

bpdufilter	Enables PortFast edge BPDU filter by default on all PortFast edge ports.
bpduguard	Enables PortFast edge BPDU guard by default on all PortFast edge ports.
edge	Enables PortFast edge mode by default on all switch access ports.
network	Enables PortFast network mode by default on all switch access ports.
normal	Enables PortFast normal mode by default on all switch access ports.

Note These keywords are available only in Cisco IOS Release 12.2(33)SXI and later releases.

Command Default

PortFast is disabled by default on all access ports.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	Mode settings (edge, network, and normal) and BPDU filter and BPDU guard settings were added.

Usage Guidelines

Caution Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the operation of the router or switch and the network.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

You can enable PortFast mode on individual interfaces using the **spanning-tree portfast** (interface) command.

Examples

This example shows how to enable PortFast by default on all access ports in releases earlier than Cisco IOS Release 12.2(33)SXI:

```
Router(config)# spanning-tree portfast default
Router(config)#
```

This example shows how to enable PortFast edge mode with BPDU Guard by default on all access ports in Cisco IOS Release 12.2(33)SXI and later releases:

```
Router(config)# spanning-tree portfast edge bpduguard default
Router(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast (interface)	Enables PortFast on a specific interface.

spanning-tree port-priority

To set an interface priority when two bridges tie for position as the root bridge, use the **spanning-tree port-priority** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

spanning-tree port-priority *port-priority*

no spanning-tree port-priority

Syntax Description

port-priority	Port priority; valid values are from 2 to 255. The default is 128.

Command Default

The port priority is 128.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on the 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 the 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.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The priority you set breaks the tie.

Examples

The following example shows how to increase the likelihood that spanning-tree instance 20 is chosen as the root-bridge on interface Ethernet 2/0:

```
Router(config)# interface ethernet 2/0
Router(config-if)# spanning-tree port-priority 20
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning-tree cost	Sets the path cost of the interface for STP calculations.
spanning-tree mst	Sets the path cost and port-priority parameters for any MST instance (including the CIST with instance ID 0).
spanning-tree portfast (global)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree portfast (interface)	Enables PortFast mode, which places the interface immediately into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree uplinkfast	Enables the UplinkFast feature.
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree transmit hold-count

To specify the transmit hold count, use the **spanning-tree transmit hold-count** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree transmit hold-count *value*

no spanning-tree transmit hold-count

Syntax Description

value	Number of bridge protocol data units (BPDUs) that can be sent before pausing for 1 second; valid values are from 1 to 20.

Command Default

value is **6**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF	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 supported on all spanning-tree modes.

The transmit hold count determines the number of BPDUs that can be sent before pausing for 1 second.

Note Changing this parameter to a higher value may have a significant impact on CPU utilization, especially in rapid-Per-VLAN Spanning Tree (PVST) mode. Lowering this parameter could slow convergence in some scenarios. We recommend that you do not change the value from the default setting.

If you change the *value* setting, enter the **show running-config** command to verify the change.

If you delete the command, use the **show spanning-tree mst** command to verify the deletion.

Examples

This example shows how to specify the transmit hold count:

```
Router(config)# spanning-tree transmit hold-count 8
Router(config)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.
show spanning-tree mst	Display the information about the MST protocol.

spanning-tree uplinkfast

To enable UplinkFast, use the **spanning-tree uplinkfast** command in global configuration mode. To disable UplinkFast, use the **no** form of this command.

spanning-tree uplinkfast [**max-update-rate** *packets-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

Syntax Description

max-update-rate *packets-per-second*	(Optional) Specifies the maximum rate (in packets per second) at which update packets are sent; valid values are from 0 to 65535.

Command Default

The defaults are as follows:

- UplinkFast is disabled.
- *packets-per-second* is 150 packets per second.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command only on access switches.

When you configure UplinkFast, the bridge priority is changed to 49152 so that this switch is not selected as root. All interface path costs of all spanning-tree interfaces that belong to the specified spanning-tree instances also increase by 3000.

When spanning tree detects that the root interface has failed, UplinkFast causes an immediate switchover to an alternate root interface, transitioning the new root interface directly to the forwarding state. During this time, a topology change notification is sent. To minimize the disruption that is caused by the topology change, a multicast packet is sent to 01-00-0C-CD-CD-CD for each station address in the forwarding bridge except for those associated with the old root interface.

Use the **spanning-tree uplinkfast max-update-rate** command to enable UplinkFast (if it is not already enabled) and change the rate at which update packets are sent. Use the **no** form of this command to return to the default rate.

Examples

This example shows how to enable UplinkFast and set the maximum rate to 200 packets per second:

```
Router(config)# spanning-tree uplinkfast max-update-rate 200
Router(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree vlan

To configure Spanning Tree Protocol (STP) on a per-virtual LAN (VLAN) basis, use the **spanning-tree vlan** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree vlan *vlan-id* [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **protocol** *protocol* | [**root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]]

no spanning-tree vlan *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **protocol** | **root**]

Syntax Description

vlan-id	VLAN identification number; valid values are from 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.
forward-time *seconds*	(Optional) Sets the STP forward delay time; valid values are from 4 to 30 seconds.
hello-time *seconds*	(Optional) Specifies the duration, in seconds, between the generation of configuration messages by the root switch; valid values are from 1 to 10 seconds.
max-age *seconds*	(Optional) Sets the maximum number of seconds the information in a bridge packet data unit (BPDU) is valid; valid values are from 6 to 40 seconds.
priority *priority*	(Optional) Sets the STP bridge priority; valid values are from 0 to 65535.
protocol *protocol*	(Optional) Sets the STP. See the "Usage Guidelines" section for a list of valid values.
root primary	(Optional) Forces this switch to be the root bridge.
root secondary	(Optional) Specifies this switch to act as the root switch should the primary root fail.
diameter *net-diameter*	(Optional) Specifies the maximum number of bridges between any two points of attachment of end stations; valid values are from 2 through 7.

Command Default

The defaults are:

- **forward-time**—15 seconds
- **hello-time**—2 seconds
- **max-age**—20 seconds
- **priority**—The default with IEEE STP enabled is 32768; the default with STP enabled is 128.
- **protocol**—IEEE
- **root**—No STP root

When you issue the **no spanning-tree vlan** *xx* **root** command the following parameters are reset to their defaults:

- **priority**—The default with IEEE STP enabled is 32768; the default with STP enabled is 128.
- **hello-time**—2 seconds

- **forward-time**—15 seconds
- **max-age**—20 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	Support for this command on the Catalyst 6000 series switches was extended to Cisco IOS Release 12.1(1)E.
12.2(2)XT	This command was implemented on the 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 the 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.
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(33)SRA	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 1–4094 for specified platforms.

Usage Guidelines

Caution When disabling spanning tree on a VLAN using the **no spanning-tree vlan** *vlan-id* command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.

Caution We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

When you set the **max-age** *seconds* parameter, if a bridge does not hear bridge protocol data units (BPDUs) from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.

Valid values for *protocol* are **dec** (Digital STP), **ibm** (IBM STP), **ieee** (IEEE Ethernet STP), and **vlan-bridge** (VLAN Bridge STP).

The **spanning-tree root primary** command alters this switch's bridge priority to 8192. If you enter the **spanning-tree root primary** command and the switch does not become the root switch, then the bridge priority is changed to 100 less than the bridge priority of the current bridge. If the switch still does not become the root, an error results.

The **spanning-tree root secondary** command alters this switch's bridge priority to 16384. If the root switch should fail, this switch becomes the next root switch.

Use the **spanning-tree root** commands on backbone switches only.

The **spanning-tree etherchannel guard misconfig** command detects two types of errors: misconfiguration and misconnection errors. A misconfiguration error is an error between the port-channel and an individual port. A misconnection error is an error between a switch that is channeling more ports and a switch that is not using enough Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) to detect the error. In this case, the switch will only error disable an EtherChannel if the switch is a nonroot switch.

Examples

The following example shows how to enable spanning tree on VLAN 200:

```
Router(config)# spanning-tree vlan 200
```

The following example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Router(config)# spanning-tree vlan 10 root primary diameter 4
```

The following example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Router(config)# spanning-tree vlan 10 root secondary diameter 4
```

Related Commands

Command	Description
spanning-tree cost	Sets the path cost of the interface for STP calculations.
spanning-tree etherchannel guard misconfig	Displays an error message when a loop due to a channel misconfiguration is detected
spanning-tree port-priority	Sets an interface priority when two bridges tie for position as the root bridge.
spanning-tree portfast (global)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire.
spanning-tree portfast (interface)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire.
spanning-tree uplinkfast	Enables the UplinkFast feature.
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.

udld

To enable aggressive or normal mode in UniDirectional Link Detection protocol (UDLD) and set the configurable message time, use the **udld** command in global configuration mode. To disable aggressive or normal mode in UDLD, use the **no** form of this command.

udld {**aggressive | enable | message time** *seconds*}

no udld {**aggressive | enable | message time** *seconds*}

Syntax Description

enable	Enables UDLD in normal mode by default on all fiber interfaces.
aggressive	Enables UDLD in aggressive mode by default on all fiber interfaces.
message time *seconds*	Sets the period of time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 7 to 90 seconds.

Command Default

The defaults are as follows:

- UDLD is disabled on all fiber interfaces.
- *seconds* is 15 seconds.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

- Disable normal-mode UDLD on all fiber ports by default.
- Disable aggressive-mode UDLD on all fiber ports by default.
- Disable the message timer.

If you enable aggressive mode, after all the neighbors of a port age out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to resynchronize with any potentially out-of-sync neighbor and shuts down the port if the message train from the link is still undetermined.

This command affects fiber interfaces only. Use the **udld port** command in interface-configuration mode to enable UDLD on other interface types.

Examples

This example shows how to enable UDLD on all fiber interfaces:

```
Router(config)# udld enable
Router(config)#
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD status.
udld port	Enables UDLD on the interface or enables UDLD in aggressive mode on the interface.

udld port

To enable the Unidirectional Link Detection (UDLD) protocol on the interface or enable UDLD in aggressive mode on the interface, use the **udld port** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

udld port [**aggressive**]

no udld port [**aggressive**]

Syntax Description

aggressive	(Optional) Enables UDLD in aggressive mode on this interface; see the "Usage Guidelines" section for additional information.

Command Default

The defaults are as follows:

- Fiber interfaces are in the state of the global **udld** (**enable** or **aggressive**) command.
- Nonfiber interfaces have UDLD disabled.

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(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.

Usage Guidelines

This command does not appear in the CLI unless a GBIC is in the port that you are trying to enable.

Use the **udld port** and **udld port aggressive** commands on fiber ports to override the setting of the global **udld** (**enable** or **aggressive**) command. Use the **no** form on fiber ports to remove this setting and return control of UDLD enabling back to the global **udld** command, or in the case of nonfiber ports, to disable UDLD.

If you enable aggressive mode, after all the neighbors of a port age out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to resynchronize with any potentially out-of-sync neighbor and shuts down the port if the message train from the link is still undetermined.

If the port changes from fiber to nonfiber or vice versa, all configurations are maintained because the platform software detects a change of module or a Gigabit Interface Converter (GBIC) change.

Examples

This example shows how to cause any port interface to enable UDLD regardless of the current global **udld** setting:

```
Router(config-if)# udld port
Router(config-if)#
```

This example shows how to cause any port interface to enable UDLD in aggressive mode regardless of the current global **udld** (**enable** or **aggressive**) setting:

```
Router(config-if)# udld port aggressive
Router(config-if)#
```

This example shows how to cause a fiber port interface to disable UDLD regardless of the current global **udld** setting:

```
Router(config-if)# no udld port
Router(config-if)#
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD status.
udld	Enables aggressive or normal mode in UDLD and sets the configurable message time.

udld reset

To reset all the ports that are shut down by the Unidirectional Link Detection (UDLD) protocol and permit traffic to begin passing through them again (although other features, such as spanning tree, Port Aggregation Protocol [PAgP], and Dynamic Trunking Protocol [DTP], will behave normally if enabled), use the **udld reset** command, in privileged EXEC mode.

udld reset

Syntax Description

This command has no arguments or keywords.

Command Default

Ports shut down are not reset.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports will begin to run UDLD again and may shut down for the same reason if the reason for the shutdown has not been corrected.

Examples

This example shows how to reset all ports that are shut down by UDLD:

```
Router# udld reset
Router#
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD status.

vlan (global)

To add a VLAN and enter config-VLAN submode, use the **vlan** command in global configuration mode. To delete the VLAN, use the **no** form of this command.

vlan {*vlan-id* | *vlan-range*}

no vlan {*vlan-id* | *vlan-range*}

Syntax Description

vlan-id	Number of the VLAN; valid values are from 1 to 4094. See the "Usage Guidelines" section for details on configuring VLAN ID numbers.
vlan-range	Range of configured VLANs; see the "Usage Guidelines" section for details on configuring ranges of VLAN ID numbers.

Defaults

This command has no default settings.

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 integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

VLAN 1 and VLANs 1002–1005 are default VLANs. Default VLANs are created automatically and cannot be configured or deleted by users.

The specified VLAN is added or modified in the VLAN database when you exit config-VLAN submode.

When you enter the **vlan** *vlan-id* command, a new VLAN is created with all default parameters in a temporary buffer and causes the CLI to enter config-VLAN submode. If the *vlan-id* that you entered matches an existing VLAN, any configuration commands you enter in config-VLAN submode will apply to the existing VLAN. You will not create a new VLAN.

If you define a range of configured VLANS, you are not allowed to set the *vlan-name* argument in config-VLAN submode.

You can enter the *vlan-range* argument using a comma (**,**), a dash (**-**), and the number.

VLAN IDs in the range from 1006 to 4094 are considered "extended VLAN IDs." Beginning in Cisco IOS Release 12.4(15)T, you can configure extended VLAN IDs on the following routers:

- Cisco 800 series routers, including models 851, 857, 871, 876, 877, 878
- Cisco 1700 series routers, including models 1711, 1712, 1751, 1751V, 1760

- Cisco 1800 series routers, including models 1801, 1802, 1803, 1811, 1812, 1841
- Cisco 2600 series routers, including models 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, 2691
- Cisco 2800 series routers, including models 2801, 2811, 2821, 2851
- Cisco 3600 series routers, including models 3620, 3640, 3640A, 3660
- Cisco 3700 series routers, including models 3725, 3745
- Cisco 3800 series routers, including models 3825, 3845

The reduced MAC address feature is required to support 4000 VLANs. Cisco IOS Release 12.1(14)E1 and later releases support chassis with 64 or 1024 MAC addresses. For chassis with 64 MAC addresses, Spanning Tree Protocol (STP) uses the extended system ID (which is the VLAN ID) plus a MAC address to make the bridge ID unique for each VLAN. (Without the reduced MAC address support, 4096 VLANs would require 4096 MAC addresses on the switch.)

If you configure extended VLANs, you must also enable the spanning-tree extended system-ID feature.

The legacy **vlan database** mode does not support extended VLAN configuration.

See the **vlan (config-VLAN)** command for information on the commands that are available under config-VLAN submode.

Examples

This example shows how to add a new VLAN and enter config-VLAN submode:

```
Router(config)# vlan 2
Router(config-vlan)#
```

This example shows how to add a range of new VLANs and enter config-VLAN submode:

```
Router(config)# vlan 2,5,10-12,20,25,4000
Router(config-vlan)#
```

This example shows how to delete a VLAN:

```
Router(config)# no vlan 2
Router(config)#
```

Related Commands

Command	Description
vlan (config-VLAN)	Configures a specific VLAN.

vlan (VLAN)

To configure a specific VLAN, use the **vlan** command in VLAN configuration mode. To delete a VLAN, use the **no** form of this command.

vlan *vlan-id* [**are** *hops*] [**backupcrf** *mode*] [**bridge** *type* | *bridge-number*] [**media** *type*] [**mtu** *mtu-size*] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *sa-id-value*] [**state** {**suspend** | **active**}] [**stp type** *type*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

no vlan *vlan-id*

Syntax Description

vlan-id	Number of the VLAN; valid values are from 2 to 1001.
are *hops*	(Optional) Specifies the maximum number of All Route Explorer hops for this VLAN. Valid values are from 0 to 13. Zero is assumed if no value is specified.
backupcrf *mode*	(Optional) Enables or disables the backup concentrator relay function (CRF) mode of the VLAN; valid values are **enable** or **disable**.
bridge *type* | *bridge-number*	(Optional) Specifies the bridging characteristics of the VLAN or identification number of the bridge; valid type values are **srb** or **srt**. Valid *bridge-number* values are from 0 to 15.
media *type*	(Optional) Specifies the media type of the VLAN; valid values are **ethernet**, **fd-net**, **fddi**, **trcrf**, and **trbrf**.
mtu *mtu-size*	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
name *vlan-name*	(Optional) Defines a text string used as the name of the VLAN (1 to 32 characters).
parent *parent-vlan-id*	(Optional) Specifies the ID number of the parent VLAN for FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
ring *ring-number*	(Optional) Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
said *sa-id-value*	(Optional) Specifies the security association identifier; valid values are from 1 to 4294967294
state {**suspend** | **active**}	(Optional) Specifies whether the state of the VLAN is active or suspended. VLANs in suspended state do not pass packets.
stp type *type*	(Optional) Specifies the Spanning Tree Protocol (STP) type; valid values are **ieee**, **ibm**, and **auto**.
tb-vlan1 *tb-vlan1-id*	(Optional) Specifies the ID number of the first translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is the default value.
tb-vlan2 *tb-vlan2-id*	(Optional) Specifies the ID number of the second translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is the default value.

Command Default

The defaults are as follows:

- *vlan-name*—VLAN*xxxx* where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **media** *type*—ethernet.

- **state**—Active.
- *said-value*—100000 plus the VLAN ID number.
- *mtu-size*—dependent upon the VLAN type:
  - ethernet—1500
  - fddi—1500
  - trcrf—1500 if V2 is not enabled, 4472 if it is enabled
  - fd-net—1500
  - trbrf—1500 if V2 is not enabled, 4472 if it is enabled
- *ring-number*—No ring number is specified.
- *bridge-number*—No bridge number is specified.
- *parent-vlan-id*—No parent VLAN is specified.
- *type*—No STP type is specified.
- **tb-vlan1** and **tb-vlan2**—0, which means no translational bridge VLAN is specified.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	Support for this command on the Catalyst 6000 series switch was extended to the E train.
12.2(2)XT	This command was implemented on the 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 the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX train.

Usage Guidelines

This command was replaced by the **vlan (config-VLAN)** command but is kept for backward compatibility.

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

This command, which is similar to the VLAN 1 parameters, are configured at the factory and cannot be changed.

Extended-range VLANs are not supported in VLAN configuration mode.

When you define *vlan-name*, the name must be unique within the administrative domain.

The security association ID (SAID) is documented in 802.10. When the **no** form is used, the VLAN's SAID is returned to the default value.

When you define the *said-value*, the name must be unique within the administrative domain.

The *bridge-number* argument is used only for Token Ring-net and FDDI-net VLANs and is ignored in other types of VLANs. When the **no** form is used, the VLAN's source-routing bridge number returns to the default value.

The parent VLAN resets to the default if the parent VLAN is deleted or the media keyword changes the VLAN type or the VLAN type of the parent VLAN.

The **tb-vlan1** and **tb-vlan2** keywords are used to configure translational bridge VLANs of a specified type and are not allowed in other types of VLANs. Translational bridge VLANs must differ in type from the affected VLAN; if two VLANs are specified, the two must be different VLAN types.

A translational bridge VLAN resets to the default if the translational bridge VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the corresponding translational bridge VLAN.

Examples

The following example shows how to add a new VLAN with all default parameters to the new VLAN database:

```
Router(vlan)# vlan 2
```

Note If the VLAN already exists, no action occurs.

The following example shows how to cause the device to add a new VLAN, specify the media type and parent VLAN ID number 3, and set all other parameters to the defaults:

```
Router(vlan)# vlan 2 media ethernet parent 3

VLAN 2 modified:
    Media type ETHERNET
    Parent VLAN 3
```

The following example shows how to delete VLAN 2:

```
Router(vlan)# no vlan 2
```

The following example shows how to return the maximum transmission unit (MTU) to the default for its type and return translational bridging VLANs to the default:

```
Router(vlan)# no vlan 2 mtu tb-vlan1 tb-vlan2
```

Related Commands

Command	Description
show vlan	Displays VLAN information.
vlan database	Enters VLAN configuration mode.

vlan access-log

To configure the VLAN access control list (VACL)-logging properties, including the log-table size, redirect-packet rate, and logging threshold, use the **vlan access-log** command in global configuration. To return to the default settings, use the **no** form of this command.

vlan access-log {**maxflow** *max-number* | **ratelimit** *pps* | **threshold** *pkt-count*}

no vlan access-log {**maxflow** | **ratelimit** | **threshold**}

Syntax Description

maxflow *max-number*	Specifies the maximum log-table size. Valid values are from 0 to 2048; 0 deletes the contents of the log table.
ratelimit *pps*	Specifies the maximum redirect VACL-logging packet rate; valid values are from 0 to 5000.
threshold *pkt-count*	Specifies the logging-update threshold; valid values are from 0 to 2147483647. 0 means that the threshold is not set.

Command Default

The defaults are as follows:

- *max-number* is **500**.
- *pps* is **2000** pps.
- *pkt-count* is not set.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Due to the rate-limiting function for redirected packets, VACL-logging counters may not be accurate.

Only denied IP packets are logged.

When the log-table size is full, the logging packets from the new flows are dropped by the software.

The packets that exceed the maximum redirect VACL-logging packet rate limit are dropped by the hardware.

A logging message is displayed if the flow threshold is reached before the 5-minute interval.

If you do not configure the maximum log-table size, maximum packet rate, or threshold, or if you enter the **no** form of the commands, the default values are assumed.

Examples

This example shows how to set the maximum log-table size:

```
Router(config)# vlan access-log maxflow 500
Router(config)#
```

This example shows how to set the maximum redirect VACL-logging packet rate after which packets are dropped:

```
Router(config)# vlan access-log ratelimit 200
Router(config)#
```

This example shows how to set the logging-update threshold:

```
Router(config)# vlan access-log threshold 3500
Router(config)#
```

Related Commands

Command	Description
show vlan access-log	Displays information about the VACL logging including the configured logging properties.

vlan access-map

To create a VLAN access map or enter VLAN access-map command mode, use the **vlan access-map** command in global configuration. To remove a mapping sequence or the entire map, use the **no** form of this command.

vlan access-map *name* [*seq-number*]

no vlan access-map *name* [*seq-number*]

Syntax Description

name	VLAN access-map tag.
seq-number	(Optional) Map sequence number; valid values are 0 to 65535.

Command Default

A VLAN access map is not created.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you enter the sequence number of an existing map sequence, you enter VLAN access-map mode.

If you do not specify a sequence number, a number is automatically assigned. You can enter one match clause and one action clause per map sequence.

If you enter the **no vlan access-map name** [*seq-number*] command without entering a sequence number, the whole map is removed.

Once you enter VLAN access-map mode, the following commands are available:

- **action**—Specifies the packet action clause; see the **action** command section.
- **default**—Sets a command to its defaults.
- **end**—Exits from configuration mode.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Specifies the match clause; see the **match** command section.
- **no**—Negates a command or sets its defaults.

Examples

This example shows how to enter VLAN access-map mode:

```
Router(config)# vlan access-map tagname1
Router(config-access-map)#
```

Related Commands

Command	Description
action	Sets the packet action clause.
match	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
show vlan access-map	Displays the contents of a VLAN-access map.

vlan accounting

To configure accounting information about VLAN, use the **vlan accounting** command in global configuration mode. To remove the accounting information, use the **no** form of this command.

vlan accounting {**input | output**}

no vlan accounting {**input | output**}

Syntax Description

input	Specifies the incoming accounting information.
output	Specifies the outgoing accounting information.

Command Default

The accounting information about VLAN is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to configure incoming accounting information about VLAN:

```
Router# enable
Router# configure terminal
Router(config)# vlan accounting input
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

vlan database

Note The **vlan database** command is not available in Cisco IOS Release 12.2(33)SXI5 and later Cisco IOS 12.2SX releases.

To enter VLAN configuration mode, use the **vlan database** command in privileged EXEC mode.

vlan database

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN configuration mode is not entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6500 series switches.
12.1(1)E	Support for this command on the Catalyst 6500 series switches was extended to the E release.
12.2(2)XT	This command was implemented on the 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 the 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.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note If you are running in RPR+ mode on a Cisco 7600 series router or Catalyst 6500 series switch, do not configure a VLAN in VLAN-database mode. Performance problems might occur during configuration synchronization between the active and standby supervisor engines.

Once you are in VLAN configuration mode, you can access the VLAN database editing buffer manipulation commands, including:

- **abort**—Exits themode without applying the changes.
- **apply**—Applies current changes and increases the release number.
- **exit**—Applies changes, increases the release number, and exit mode.

- **no**—Negates a command or sets its defaults; valid values are **vlan** and **vtp**.
- **reset**—Abandons current changes and rereads the current database.
- **show**—Displays database information.
- **vlan**—Accesses subcommands to add, delete, or modify values associated with a single VLAN. For information about the **vlan** subcommands, see the **vlan** (VLAN) command.
- **vtp**—Accesses subcommands to perform Virtual Trunking Protocol (VTP) administrative functions. For information about the **vtp** subcommands, see the **vtp client** command.

Examples

The following example shows how to enter VLAN configuration mode:

```
Router# vlan database
Router(vlan)#
```

The following example shows how to exit VLAN configuration mode without applying changes after you are in VLAN configuration mode:

```
Router(vlan)# abort
Aborting....
Router#
```

The following example shows how to delete a VLAN after you are in VLAN configuration mode:

```
Router(vlan)# no vlan 100
Deleting VLAN 100...
Router(vlan)#
```

This example shows how to delete a VLAN after you are in VLAN-configuration mode:

```
Router(vlan)# no vlan 100
Deleting VLAN 100...
Router(vlan)#
```

This example shows how to turn off pruning after you are in VLAN-configuration mode:

```
Router(vlan)# no vtp pruning
Pruning switched OFF
Router(vlan)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

vlan dot1q tag native

To enable dot1q (802.1Q) tagging for all VLANs in a trunk, use the **vlan dot1q tag native** command in global configuration mode. To clear the configuration, use the **no** form of this command.

vlan dot1q tag native

no vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Command Default

Dot1q (802.1Q) tagging for all VLANs in a trunk is disabled.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **vlan dot1q tag native** command configures the switch to tag native-VLAN traffic and admit only 802.1Q-tagged frames on 802.1Q trunks, dropping any untagged traffic, including untagged traffic in the native VLAN.

Follow these configuration guidelines when configuring Layer 2-protocol tunneling:

- On all the service-provider edge switches, you must enable spanning-tree bridge protocol data unit (BPDU) filtering on the 802.1Q-tunnel ports by entering the **spanning-tree bpdufilter enable** command.
- Ensure that at least one VLAN is available for native-VLAN tagging. If you use all the available VLANs and then enter the **vlan dot1q tag native** command, native-VLAN tagging is not enabled.
- On all the service-provider core switches, enter the **vlan dot1q tag native** command to tag native-VLAN egress traffic and drop untagged native-VLAN ingress traffic.
- On all the customer switches, either enable or disable native-VLAN tagging on each switch.

Note If you enable dot1q tagging on one switch and disable it on another switch, all traffic is dropped; you must identically configure dot1q tagging on each switch.

Examples

This example shows how to enable dot1q tagging for all VLANs in a trunk:

```
Router(config)# vlan dot1q tag native
Router(config)#
```

Related Commands

Command	Description
show vlan dot1q tag native	Displays native VLAN-tagging information.

vlan filter

To apply a VLAN access map, use the **vlan filter** command in global configuration mode. To clear the VLAN access maps from VLANs or interfaces, use the **no** form of this command.

vlan filter *map-name* {**vlan-list** *vlan-list* | **interface** *interface interface-number*}

no vlan filter *map-name* {**vlan-list** [*vlan-list*] | **interface** [*interface interface-number*]}

Syntax Description

map-name	VLAN access-map tag.
vlan-list	VLAN list; valid values are from 1 to 4094. See the "Usage Guidelines" section for additional information on the *vlan-list* argument.
interface *interface*	Specifies the interface type; valid values are **pos**, **atm**, or **serial**. See the "Usage Guidelines" section for additional information.
interface-number	Interface number; see the "Usage Guidelines" section for additional information.

Command Default

A VLAN access map is not applied.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When configuring an action clause in a VLAN access map, note the following:

- You can apply the VLAN access map to one or more VLANs or WAN interfaces.
- The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by a hyphen (-) or a comma (,).
- If you delete a WAN interface that has a VLAN access control list (VACL) applied, the VACL configuration on the interface is also removed.
- You can apply only one VLAN access map to each VLAN or WAN interface.
- VACLs that are applied to VLANs are active only for VLANs with a Layer 3-VLAN interface configured. VACLs that are applied to VLANs without a Layer 3-VLAN interface are inactive. Applying a VLAN access map to a VLAN without a Layer 3-VLAN interface creates an administratively down Layer 3-VLAN interface to support the VLAN access map. If creation of the Layer 3-VLAN interface fails, the VACL is inactive.

When entering the **no** form of this command, the *vlan-list* argument is optional (but the keyword **vlan-list** is required). If you do not enter the *vlan-list* argument, the VACL is removed from all VLANs where the *map-name* argument is applied.

When entering the **no** form of this command for WAN interfaces, the *interface* argument is optional (but the **interface** keyword is required). If you do not enter the *interface* argument, the VACL is removed from interfaces where the *map-name* is applied.

The **vlan filter** *map-name* **interface** command accepts only ATM, POS, or serial interface types. If your Catalyst 6500 series switch is not configured with any of these interface types, the **interface** *interface interface-number* keyword and argument are not provided.

The *interface-number* format can be *mod*/*port* or *slot*/*port-adapter*/*port*; it can include a subinterface or channel-group descriptor.

Examples

This example shows how to apply a VLAN access map on VLANs 7 through 9:

```
Router(config)# vlan filter ganymede vlan-list 7-9
Router(config)#
```

Related Commands

Command	Description
action	Sets the packet action clause.
match	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
show vlan filter	Displays information about the VLAN filter.

vlan ifdescr detail

To enable the Cisco device to provide detailed display information for VLAN subinterfaces in ifDescr format, use the **vlan ifdescr detail** command in global configuration mode. To disable this functionality, use the **no** form of this command.

vlan ifdescr detail

no vlan ifdescr detail

Syntax Description

This command has no arguments or keywords.

Command Default

Information about VLAN subinterfaces is not displayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to enable the display information for VLAN interfaces:

```
Router# configure terminal
Router(config)# vlan ifdescr detail
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

vlan internal allocation policy

To configure the allocation direction of the internal VLAN, use the **vlan internal allocation policy** command in global configuration mode. To the default setting, use the **no** form of this command to return.

vlan internal allocation policy {**ascending | descending**}

no vlan internal allocation policy

Syntax Description

ascending	Allocates internal VLANs from 1006 to 4094.
descending	Allocates internal VLANs from 4094 to 1006.

Command Default

ascending

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can configure internal VLAN allocation to be from 1006 and up or from 4094 and down.

Internal VLANs and user-configured VLANs share the 1006 to 4094 VLAN spaces. A “first come, first served” policy is used in allocating these spaces.

You must perform a system reboot before the **vlan internal allocation policy** command changes can take effect.

During system bootup, internal VLANs that are required for features in the startup-config file are allocated first. The user-configured VLANs in the startup-config file are configured next. If you configure a VLAN that conflicts with an existing internal VLAN, the VLAN that you configured is put into a nonoperational status until the internal VLAN is freed and becomes available.

After you enter the **write mem** command and the system reloads, the reconfigured allocation is used by the port manager.

Examples

This example shows how to configure VLANs in a descending order as the internal VLAN-allocation policy:

```
Router(config)# vlan internal allocation policy descending
Router(config)#
```

Related Commands

Command	Description
show vlan internal usage	Displays information about the internal VLAN allocation.

vlan mapping dot1q

To map an 802.1Q VLAN to an Inter-Switch Link (ISL) VLAN, use the **vlan mapping dot1q** command in global configuration mode. To remove a specified mapping or all 802.1Q VLAN-to-ISL VLAN mappings, use the **no** form of this command.

vlan mapping dot1q *dot1q-vlan-id* **isl** *isl-vlan-id*

no vlan mapping {**dot1q** *dot1q-vlan-id* | **all**}

Syntax Description

dot1q *dot1q-vlan-id*	Specifies the VLAN ID of the 802.1Q VLAN from which the mapping occurs as traffic leaves and enters 802.1Q trunks on the local device; valid values are from 1 to 4094.
isl *isl-vlan-id*	Specifies the VLAN ID of the ISL VLAN onto which the mapping occurs as traffic leaves and enters 802.1Q trunks on the local device and specifies the VLAN ID of the 802.1Q VLAN for which to discard traffic as it arrives at a local device; valid values are from 1 to 4094.
all	Removes all 802.1Q VLAN-to-ISL VLAN mappings.

Command Default

The default for 802.1Q VLAN IDs 1 to 4094 is an identity mapping.

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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

You can map up to eight VLANs. You can map only one 802.1Q VLAN to an ISL VLAN. For example, if 802.1Q VLAN 800 has been automatically mapped to ISL VLAN 800, do not manually map any other 802.1Q VLANs to ISL VLAN 800.

You cannot overwrite existing 802.1Q-VLAN mapping. If the 802.1Q-VLAN number already exists, the command is aborted. You must first clear that mapping.

If the table is full, the command is aborted with an error message indicating that the table is full.

Examples

This example shows how to map traffic arriving on 802.1Q trunks on VLAN 1001 to ISL VLAN 888 on the local device, discard traffic arriving on 802.1Q trunks on VLAN 888, and map traffic on ISL VLAN 888 on the local device to 802.1Q VLAN 1001 as it leaves the device:

```
Router(config)# vlan mapping dot1q 1001 isl 888
Router(config)#
```

This example shows how to clear the mapping of 802.1Q VLAN 1001 to ISL VLAN 888. The result is that 802.1Q VLAN 1001 traffic is discarded when it arrives on the local device, and 802.1Q VLAN 888 traffic is mapped to ISL VLAN 888 (both are their default states):

```
Router(config)# no vlan mapping dot1q 1001
No mapping for 1022
Router(config)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.
vlan (VLAN)	Configures a specific VLAN.
vlan database	Enters VLAN-configuration submode.

vlan port provisioning

To enable VLAN port provisioning verification, use the **vlan port provisioning** command in global configuration mode. To disable VLAN port provisioning verification, use the **no** form of this command.

vlan port provisioning

no vlan port provisioning

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN port provisioning verification is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

When you enable the VLAN port provisioning, you must specify the VLAN name in order to change a port from one VLAN to another.

When VLAN port provisioning is enabled, you can still create new VLANs, but you cannot add ports to the VLAN without specifying both the VLAN number and the VLAN name. The feature does not affect assigning ports to VLANs using other features such as Simple Network Management Protocol (SNMP), dynamic VLANs, and 802.1X.

Examples

The following example shows how to enable VLAN port provisioning on all ports:

```
Router(config)# vlan port provisioning
```

The following example shows how to disable VLAN port provisioning on all ports:

```
Router(config)# no vlan port provisioning
```

Related Commands

Command	Description
show vlan port provisioning	Displays the VLAN port provisioning status.

vtp (global)

To configure the global VLAN Trunking Protocol (VTP) state, use the **vtp** command in global configuration mode. To return to the default value, use the **no** form of this command.

vtp {**domain** *domain-name* | **file** *filename* | **interface** *interface-name* [**only**] | **mode** {**client** | **off** | **server** | **transparent**} | **password** *password-value* | **pruning** | **version** {**1** | **2**}}

no vtp

Catalyst 6500 Series Switch

vtp {**domain** *domain-name* | **file** *filename* | **interface** *interface-name* [**only**] | **mode** {**client** | **off** | **server** [**mst** | **unknown** | **vlan**] | **transparent**} | **password** *password-value* [**hidden** | **secret**] | **pruning** | **version** {**1** | **2** | **3**}}

no vtp

Syntax Description

domain *domain-name*	Sets the VTP-administrative domain name.
file *filename*	Sets the ASCII name of the IFS-file system file where the VTP configuration is stored.
interface *interface-name*	Sets the name of the preferred source for the VTP-updater ID for this device.
only	(Optional) Specifies to use only this interface's IP address as the VTP-IP updater address.
mode client	Sets the type of VTP-device mode to client mode.
mode off	Sets the type of VTP-device mode to off mode.
mode server	Sets the type of VTP-device mode to server mode.
mode transparent	Sets the type of VTP-device mode to transparent mode.
password *password-value*	Specifies the administrative-domain password.
pruning	Enables the administrative domain to permit pruning.
Catalyst 6500 Series Switch	
hidden	(Optional) Configures the password with a secret key saved in hexadecimal format in the running configuration. Supported on the Catalyst 6500 series switch only.
secret	(Optional) Allows the password secret key to be directly configured. Supported on the Catalyst 6500 series switch only.
mst	Sets the mode for Multiple Spanning-Tree (MST) VTP instance.
unknown	Sets the mode for unknown VTP features.
vlan	Sets the mode for VLAN VTP instance.
version {1 | 2 | 3}	Specifies the administrative-domain VTP-version number.

Command Default

The defaults are as follows:

- **vtp domain** and **vtp interface** commands have no default settings.
- *filename* is **const-nvram:vlan.dat**.
- VTP mode is **mode server**.
- No password is configured.
- Pruning is disabled.
- Administrative-domain VTP-version number 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	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 Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The **mode off** keyword combination was added.
12.2(33)SXI	The following changes were made for the Catalyst 6500 series switch: • **vtp mode** {**client** | **off** | **server** [**mst** | **unknown** | **vlan**] | **transparent**]} • **vtp password** *password-value* [**hidden** | **secret**] • **vtp version** {**1** | **2** | **3**}
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Note The **vtp pruning**, **vtp password**, and **vtp version** commands are also available in privileged EXEC mode. We recommend that you use these commands in global configuration mode only; do not use these commands in privileged EXEC mode.

Extended-range VLANs are not supported by VTP version 1 and version 2. Extended range VLANs are supported in VTP version 3.

When you define the *domain-name* value, the domain name is case sensitive and can be from 1 to 32 characters.

The *filename* and *interface-name* values are ASCII strings from 1 to 255 characters.

You must configure a password on each network device in the management domain when the switch is in secure mode.

Caution If you configure VTP in secure mode, the management domain does not function properly if you do not assign a management domain password to each network device in the domain.

A VTP version 2-capable network device can operate in the same VTP domain as a network device running VTP version 1 if VTP version 2 is disabled on the VTP version 2-capable network device (VTP version 2 is disabled by default).

Do not enable VTP version 2 on a network device unless all of the network devices in the same VTP domain are version 2-capable. When you enable VTP version 2 on a network device, all of the version 2-capable network devices in the domain enable VTP version 2.

In a Token Ring environment, you must enable VTP version 2 for VLAN switching to function properly.

Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.

Configuring VLANs as pruning eligible or pruning ineligible on an applicable device affects pruning eligibility for those VLANs on that switch only; it does not affect pruning eligibility on all network devices in the VTP domain.

The **vtp password**, **vtp pruning**, and **vtp version** commands are not placed in startup memory but are included in the VTP transparent-mode startup configuration file.

Extended-range VLANs are not supported by VTP.

You can configure the **pruning** keyword in VTP-server mode; the **version** keyword is configurable in VTP-server mode or VTP transparent mode.

The *password-value* argument is an ASCII string from 8 to 64 characters identifying the administrative domain for the device.

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.

All applicable devices in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on applicable devices in the same VTP domain.

If all applicable devices in a domain are VTP version 2-capable, you need only to enable VTP version 2 on one applicable devices; the version number is then propagated to the other version 2-capable applicable devices in the VTP domain.

If you toggle the version 2 mode, certain default VLAN parameters are modified.

If you enter the **vtp mode off** command, it sets the device to off. If you enter the **no vtp mode off** command, it resets the device to the VTP server mode.

Catalyst 6500 Series Switch

VTP version 3 supports all the features in version 1 and version 2. VTP version 3 also supports the following features not supported in version 1 and version 2:

- Enhanced authentication—In VTP version 3, you can configure the authentication password to be hidden using the **vtp password** command. When you configure the authentication password to be hidden, it does not appear in plain text in the configuration. Instead, the secret associated with the password is saved in hexadecimal format in the running configuration. The *password-string* argument is an ASCII string from 8 to 64 characters identifying the administrative domain for the device. The following syntax is available:

  password *password-string* [**hidden** | **secret**]

  password *password-string*—Specifies the administrative domain password.

  hidden—(Optional) Configures the password with a secret key saved in hexadecimal format in the running configuration.

secret—(Optional) Allows the password secret key to be directly configured in hexadecimal format.

The **hidden** keyword for the VTP password is supported only in VTP version 3. If converting to VTP version 2 from VTP version 3, you must remove the **hidden** keyword prior to the conversion.

- Support for extended-range VLAN database propagation—VTP version 1 and version 2 support VLANs 1 to 1000 only. In VTP version 3, the entire VLAN range is supported (VLANs 1 to 4096). The pruning of VLANs still applies to VLANs 1 to 1000 only. Extended-range VLANs are supported in VTP version 3 only. If converting from VTP version 3 to VTP version 2, VLANs in the range 1006 to 4094 are removed from VTP control.
- Support for propagation of any database in a domain—In VTP version 1 and version 2, a VTP server is used to backup the database to the NVRAM and allows you to change the database information. In VTP version 3, there is a VTP-primary server and a VTP-secondary server. A primary server allows you to alter the database information, and the database updates sent out are honored by all the devices in the system. A secondary server can only back up the updated VTP configuration received from the primary server in the NVRAMs. The status of the primary and secondary servers is a runtime status and is not configurable.

  By default, all devices come up as secondary servers. You can enter the **vtp primary** privileged EXEC mode command to specify a primary server. The following syntax is available:

  vtp primary [**vlan** | **mst**] [**force**]

  vlan—(Optional) Specifies this device as the primary server for the VTP VLAN feature.

  mst—(Optional) Specifies this device as the primary server for the VTP MST feature.

  force—(Optional) Forces this device to become the primary server.

  The primary-server status is needed only when database changes have to be performed and is obtained when the administrator issues a takeover message in the domain. The primary-server status is lost when you reload, switch over, or the domain parameters change. The secondary servers back up the configuration and continue to propagate the database. You can have a working VTP domain without any primary servers.

  In VTP version 3, there is no longer a restriction to propagate only VLAN database information. You can use VTP version 3 to propagate any database information across the VTP domain. A separate instance of the protocol is running for each application that uses VTP.
- CLI to turn off/on VTP on a per-trunk basis—You can disable VTP on a per-trunk basis using the **no vtp** command in interface configuration mode. When you disable VTP on the trunking port, all the VTP instances for that port are disabled. You will not be provided with the option of setting VTP to OFF for the MST database and ON for the VLAN database. You can enable VTP on a per-trunk basis using the **vtp** command in interface configuration mode.

  VTP on a global basis—When you set VTP mode to OFF globally, this applies to all the trunking ports in the system. Unlike the per-port configuration, you can specify the OFF option on a per-VTP instance basis. For example, the system could be configured as VTP-server for the VLAN database and as VTP-off for the MST database. In this case, VLAN databases are propagated by VTP, MST updates are sent out on the trunk ports in the system, and the MST updates received by the system are discarded.

Examples

The following example shows how to set the device's management domain:

```
Router(config)# vtp domain DomainName1
```

The following example shows how to specify the file in the IFS-file system where the VTP configuration is stored:

```
Router(config)# vtp file vtpconfig

Setting device to store VLAN database at filename vtpconfig.
```

The following example shows how to set the VTP mode to client:

```
Router(config)# vtp mode client

Setting device to VTP CLIENT mode.
```

The following example shows how to disable VTP mode globally:

```
Router(config)# vtp mode off

Setting device to VTP OFF mode.
```

The following example shows how to reset the device to the VTP server mode:

```
Router(config)# no vtp mode off

Setting device to VTP OFF mode.
```

Related Commands

Command	Description
show vtp	Displays the VTP statistics and domain information.
vtp (interface)	Enables VTP on a per-port basis.

vtp (interface)

To enable VLAN Trunking Protocol (VTP) on a per-port basis, use the **vtp** command in interface configuration mode. To disable VTP on a per-port basis, use the **no** form of this command.

vtp

no vtp

Syntax Description

This command has no arguments or keywords.

Command Default

VTP on a per-port basis is not enabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The VTP enable value is applied only when a port becomes a switched port and is in trunk mode.

Examples

This example shows how to enable VTP on a per-port basis:

```
Router(config-if)# vtp
```

This example shows how to disable VTP on a per-port basis:

```
Router(config-if)# no vtp
```

Related Commands

Command	Description
vtp mode	Globally configures VTP mode.

vtp client

To place the device in Virtual Trunking Protocol (VTP) client mode, use the **vtp client** command in VLAN configuration mode. To return to VTP server mode, use the **no** form of this command.

vtp client

no vtp client

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN mode

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on the 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 the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
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 receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch in server mode.

The **vtp server** command is the functional equivalent of **no vtp client** command except that it does not return an error if the device is not in client mode.

Examples

The following example shows how to place the device in VTP client mode:

```
Router(vlan)# vtp client
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.
vtp server	Places a device in VTP server mode.
vtp transparent	Places a device in VTP transparent mode.

vtp domain

To create the administrative domain name for the device, use the **vtp domain** command in VLAN configuration mode. To delete the administrative domain name, use the **no** form of this command.

vtp domain *domain-name*

no vtp domain

Syntax Description

domain-name	Domain name. Domain names can be a maximum of 32 characters.

Command Default

The administrative domain name is not created.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on the 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 the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
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

When you define the *domain-name* argument, the domain name is case-sensitive.

Until a domain name is set, the device is in the no-management-domain state. In this state, the device does not transmit any VLAN Trunking Protocol (VTP) advertisements regardless of changes to local VLAN configuration. The device leaves the no-management-domain state upon receiving the first VTP summary packet on any port that is currently trunking or when it receives a domain name configured by the **vtp domain** command. If the device receives its domain from a summary packet, it resets its configuration revision number to 0.

When the device leaves the no-management-domain state, it can never be configured to reenter it, except by the cleaning of NVRAM and the reloading of the device.

Examples

The following example shows how to set the device's administrative domain to DomainChandon:

```
Router(vlan)# vtp domain DomainChandon
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.

vtp password

To create a Virtual Trunking Protocol (VTP) domain password, use the **vtp password** command in VLAN configuration mode. To delete the password, use the **no** form of this command.

vtp password *password-value*

no vtp password

Syntax Description

password-value	The password. The value is an ASCII string from 1 to 32 characters.

Command Default

The default is no password.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	Support for this command on the Catalyst 6000 series switches was extended to the E train.
12.2(2)XT	This command was implemented on the 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 the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
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

The value of the *password-value* argument is an ASCII string from 1 to 32 characters.

Examples

The following example shows how to create the VTP domain password for DomainChandon:

```
Router(vlan)# vtp password DomainChandon
```

The following example shows how to delete the VTP domain password:

```
Router(vlan)# no vtp password
Clearing device VLAN database password.
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.

vtp server

To place the device in Virtual Trunking Protocol (VTP) server mode, use the **vtp server** command in VLAN configuration mode.

vtp server

Syntax Description

This command has no arguments or keywords.

Command Default

The default is VTP server mode.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	Support for this command on the Catalyst 6000 series switches was extended to the E train.
12.2(2)XT	This command was implemented on the 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 the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
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 you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all the switches in the same VTP domain.

VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

If the receiving switch is in server mode, the configuration is not changed.

The **vtp server** command is the functional equivalent of the **no vtp client** command, except that it does not return an error if the device is not in client mode.

Examples

The following example shows how to place the device in VTP server mode:

```
Router(vlan)# vtp server
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.
vtp client	Places a device in VTP client mode.
vtp transparent	Places a device in VTP transparent mode.

vtp transparent

To place the device in Virtual Trunking Protocol (VTP) transparent mode, use the **vtp transparent** command in VLAN configuration mode. To return to VTP server mode, use the **no** form of this command.

vtp transparent

no vtp transparent

Syntax Description

This command has no arguments or keywords.

Command Default

The default is VTP server mode.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	Support for this command on the Catalyst 6000 series switches was extended to the E train.
12.2(2)XT	This command was implemented on the 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 the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
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

The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.

If the receiving switch is in transparent mode, the configuration is not changed. Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to the other switches in the network.

The **vtp server** command is similar to the **no vtp transparent** command, except that it does not return an error if the device is not in transparent mode.

Examples

The following example shows how to place the device in VTP transparent mode:

```
Router(vlan)# vtp transparent
```

The following example shows how to return the device to VTP server mode:

```
Router(vlan)# no vtp transparent
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.
vtp client	Places a device in VTP client mode.
vtp server	Places a device in VTP server mode.

vtp v2-mode

To enable Virtual Trunking Protocol (VTP) version 2 mode, use the **vtp v2-mode** command in VLAN configuration mode. To disable version 2 mode, use the **no** form of this command.

vtp v2-mode

no vtp v2-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Version 2 mode is disabled.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1) E on the Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on the 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 the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
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

All switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on switches in the same VTP domain.

If all switches in a domain are VTP version 2-capable, you must enable VTP version 2 only on one switch; the version number is then propagated to the other version 2-capable switches in the VTP domain.

If you toggle the version 2 mode, parameters of certain default VLANs are modified.

Examples

The following example shows how to enable version 2 mode in the VLAN database:

```
Router(vlan)# vtp v2-mode
```

The following example shows how to disable version 2 mode in the VLAN database:

```
Router(vlan)# no vtp v2-mode
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.