bridge-domain through instance VLAN

- bridge-domain, on page 2
- bridge-domain (subinterface), on page 7
- bridge-vlan, on page 9
- clear gvrp statistics, on page 13
- clear mac-address-table, on page 14
- clear mvr counters, on page 19
- clear mvrp statistics, on page 21
- clear pagp, on page 22
- clear spanning-tree detected-protocol, on page 23
- clear vlan, on page 25
- clear vlan counters, on page 27
- clear vlan mapping, on page 28
- clear vlan statistics, on page 29
- clear vtp counters, on page 30
- collect top counters interface, on page 31
- debug udld, on page 33
- dot1q tunneling ethertype, on page 35
- efd notify, on page 37
- encapsulation dot1q, on page 38
- encapsulation isl, on page 41
- encapsulation sde, on page 42
- flowcontrol, on page 44
- flowcontrol (line), on page 46
- flowcontrol receive, on page 48
- gvrp global, on page 49
- gvrp mac-learning auto, on page 50
- gvrp registration, on page 51
- gvrp timer, on page 53
- gvrp vlan create, on page 55
- hw-module slot (ASR 1000 Series), on page 56
- instance (VLAN), on page 59
- l2protocol forward, on page 61

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.

Command Default

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.

Command	Description
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.

Command Default

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.

Command Default

- 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 **modedot1q-in-dot1qaccess-gateway** command before you can use the **bridge-vlan** command on a subinterface.

You must also use the **encapsulationdot1q** 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 **writememory** or **copyrunning-configstartup-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 *OpticalServicesModuleInstallationandConfigurationNote*.

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 **showvlaninternalusage** 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 **cleargvrpstatistics**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 **clearmac-address-table**command inprivileged EXEC mode.

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

clear mac-address-table [{**dynamic** | **restricted static** | **permanent**}] [**address** *mac-address*] [**interface** *type module port*]
clear mac-address-table notification mac-move counter [*vlan*]

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

Using Cisco ME 2600X Series Ethernet Access Switches

clear mac-address-table [{**address** *mac-address* | **interface** *interface-type interface-number* | **bridge-domain** *bridge-domain-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
bridge-domain *bridge-domain-id*	(Optional) Specifies the bridge-domain ID; valid values are from 1 to 16384.

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.

Release	Modification
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.
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 **notificationmac-movecounter** [*vlan*] keywords and argument.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

If the **clearmac-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 **clearmac-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 **clearmac-address-tabledynamic** 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-tableaging-time	Configures the length of time the switch keeps dynamic MAC addresses in memory before discarding.
mac -address-tablepermanent	Associates a permanent unicast or multicast MAC address with a particular switched port interface.
mac -address-tablerestrictedstatic	Associates a restricted static address with a particular switched port interface.
mac -address-tablesecure	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.

Command	Description
show mac -address-tablesecure	Displays the addressing security configuration.
show mac -address-tablesecurity	Displays the addressing security configuration.

clear mvr counters

To clear the join counters of all the Multicast VLAN Registration (MVR) ports, source ports, receiver ports, or of a specific MVR interface port, use the **clear mvr counters** command in privileged EXEC mode.

clear mvr counters
[**receiver-ports** | **source-ports**] | [*type module/port*]

Syntax Description

receiver-ports	Configures a port as a receiver port if it is a subscriber port. As a receiver port, it should only receive multicast data.
source-ports	Configures uplink ports that receive and send multicast data as source ports.
type	(Optional) Specifies the Interface type.
module/port	(Optional) Specifies the module or port number.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 routers.

Examples

This example shows how to clear the join counters for the receiver port on the GigabitEthernet port 1/7.

```
Router# clear mvr receiver-ports GigabitEthernet 1/7
Router# show mvr receiver-ports GigabitEthernet 1/7
Joins: v1,v2,v3 counter shows total IGMP joins
       v3 counter shows IGMP joins received with both MVR and non-MVR groups
Port   VLAN Status           Immediate            Joins
                                Leave         (v1,v2,v3)      (v3)
----   ---- -------------   ----------     ----------   -----------
Gi1/7   202 INACTIVE/UP    ENABLED                 0              0
```

Related Commands

Command	Description
mvr	Enables Multicast VLAN Registration (MVR) on the router.
mvr group	Configures an MVR group on the router.
mvr max–groups	Configures the maximum number of MVR groups on the router.

Command	Description
mvr querytime	Configures the MVR query response time.
mvr vlan	Configures the VLAN in which the multicast data is received.
mvr type	Configures a switch port as an MVR receiver or source port.
mvr immediate	Enables the immediate leave feature of the MVR on the port.
show mvr	Displays the MVR details.
show mvr groups	Displays the MVR group configuration.
show mvr interface	Displays details of all the MVR member interfaces or a single requested MVR member interface.
show mvr members	Displays details of all the MVR members and number of MVR members in all active MVR groups on a particular VLAN or port.
show mvr receiver-ports	Displays all receiver ports that are members of an IP multicast group or those on the specified interface port.
show mvr source–ports	Displays all source ports that are members of an IP multicast group or those on the specified interface port.

clear mvrp statistics

To clear statistics related to Multiple VLAN Registration Protocol (MVRP) and recorded on one (or all) MVRP-enabled ports, use the **clearmvrpstatistics** 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 **clearpagp** 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.

Command Default

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 **clearspanning-treedetected-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.

Command Default

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 **clearspanning-treedetected-protocol** command.

If you enter the **clearspanning-treedetected-protocol** command with no arguments, the command is applied to every port of the Cisco 7600 series router.

Examples

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

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

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 **clearvlan** 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 **clearvlancounters** 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.

Command Default

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
```

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 **clearvlanmapping** command in privileged EXEC mode.

clear vlan mapping dot1q{*lq-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 **clearvlanstatistics** command in privileged EXEC mode.

clear vlan statistics

Syntax Description

This command has no arguments or keywords.

Command Default

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 **clearvtpcounters** 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 **collecttopcountersinterface** 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.

Command Default

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-**collecttopcountersinterfacefastEthernetsort-byutilizationinterval***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 **showtopinterfacereport** command to view the reports. You can display the TopN reports multiple times until you enter the **cleartopinterfacereport** command to clear the reports.

Use the **cleartopinterfacereport** 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
```

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
```

Related Commands

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

debug udld

To enable the debugging of UniDirectional Link Detection (UDLD) protocol, use the **debug udld** command in the privileged EXEC mode. To disable the debugging output, use the **no** form of this command.

debug udld {**events** | **packets** | **registries**}
no debug udld {**events** | **packets** | **registries**}

Syntax Description

events	Enables debugging of UDLD process events as they occur.
packets	Enables debugging of the UDLD process as it receives packets from the packet queue and attempts to transmit packets at the request of the UDLD protocol code.
registries	Enables debugging of the UDLD process as it processes the registry upcalls from the UDLD process-dependent module and the other feature modules.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **debug udld** command is used to debug UDLD in case of any errors. The debug logs are used to analyze the error and find out where exactly the problem is occurring in UDLD.

Examples

The following is sample output from the **debug udld events** command:

```
Router# debug udld events

UDLD events debugging is on
```

The following is sample output from the **debug udld packets** command:

```
Router# debug udld packets

UDLD packets debugging is on
```

The following is sample output from the **debug udld registries** command:

```
Router# debug udld registries

UDLD registries debugging is on
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD statuses.

Command	Description
udld	Enables the aggressive mode or the normal mode in UDLD and sets the configurable message time.
udld port	Enables UDLD on the Ethernet interface or enables UDLD in the aggressive mode on the Ethernet interface.
udld recovery	Enables the recovery timer for the UDLD error-disabled state.
udld reset	Resets all the LAN ports that are error disabled by UDLD.

dot1q tunneling ethertype

To define the Ethertype field type used by peer devices when implementing Q-in-Q VLAN tagging, use the **dot1qtunnelingethertype**command in interface configuration mode. To remove the VLAN tag Ethertype, use the **no** form of this command.

no dot1q tunneling ethertype{*0x88A8 0x9100 0x9200*}
no dot1q tunneling ethertype

Syntax Description

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

Command Default

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 **dot1qtunnelingethertype** 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 **encapsulationdot1q** 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.

efd notify

To enable G.8032 or Resilient Ethernet Protocol (REP) notifications, use the **efd notify** command in Ethernet Connectivity Fault Management (CFM) service instance configuration mode. To disable G.8032 or REP notifications, use the **no** form of this command.

efd notify {**g8032** | **rep**}
no efd notify {**g8032** | **rep**}

Syntax Description

g8032	Enables G.8032 notifications if any failures are detected on the monitored links.
rep	Enables REP notifications if any failures are detected on the monitored links.

Command Default

Command Modes

CFM service instance configuration (config-ecfm-srv)

Command History

Release	Modification
Cisco IOS XE Release 13.3	This command was introduced.

Usage Guidelines

Either G.8032 or REP notifications can be configured at an instance. For example, if REP notifications are enabled while G.8032 otifications are enabled, the G.8032 notifications are disabled.

Examples

This example shows how to configure REP notifications:

```
Device(config-ecfm-srv)# efd notify rep
```

You can verify your settings by entering the **showinterfacesrepdetail**command in privileged EXEC command.

Related Commands

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

encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN, use the **encapsulationdot1q** 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** {**from-bd** | **any***vlan-idvlan-id-vlan-id* | [{,*vlan-id-vlan-id*}]}
no encapsulation dot1q *vlan-id* **second-dot1q** {**from-bd** | **any***vlan-idvlan-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.
from-bd	Configures trunk EFP with encapsulation from bridge domain (BD). In this case all the BDs configured on the switch will be part of the VLAN list of the trunk EFP configured with this command.
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.

Command Default

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.

Release	Modification
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.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.
Cisco IOS XE Everest Release 16.7.1	The **from-bd** keyword is added to configure trunk EFP with encapsulation from bridge domain (BD).

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 **encapsulationdot1q**command in interface range configuration mode to apply a VLAN ID to each subinterface within the range specified by the**interfacerange** 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 **interfacerange** 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 **encapsulationdot1q**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 **encapsulationisl** 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 **encapsulationsde** 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 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**}

Syntax Description

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.

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.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	This command was introduced 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.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

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 the **receive**keyword, 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 **sendon** only when remote ports are set to **receiveon** or **receivedesired**.
- Use **sendoff** only when remote ports are set to **receiveoff** or **receivedesired**.
- Use **receiveon** only when remote ports are set to **sendon** or **senddesired**.
- Use **sendoff** only when remote ports are set to **receiveoff** or **receivedesired**.

Examples

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

```
Router# configure terminal

Router(config)# interface GigabitEthernet1/9 10.4.9.157 255.255.255.0

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

Related Commands

Command	Description
show interfaces flowcontrol	Displays flow-control information.

flowcontrol (line)

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**}]}

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** c auses the Cisco IOS software to listen to flow control from the attached device, and the **out**keywordc auses 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.

Command Default

Flow control is disabled.

Command Modes

Line configuration (config-line)

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.

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.

Examples

The following example sets hardware flow control on line 7:

```
Router# configure terminal

Router(config)# line 7

Router(config-line)# flowcontrol hardware
```

Related Commands

Command	Description
start-character	Sets the flow control start character.
stop-character	Sets the flow control stop character.

flowcontrol receive

To temporarily stop the transmission of data between two peers to prevent packet drops in the event of data overflow , use the **flowcontrolreceive** 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

off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.

Command Default

Flow control is enabled.

Command Modes

Interface configuration (config-if)

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.

Usage Guidelines

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

Examples

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
```

gvrp global

To enable Generic VLAN Registration Protocol (GVRP) globally on a device and on an interface, use the **gvrpglobal**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 **gvrpmac-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 globallly 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

Toset the registrars in a global information distribution (GID) instance associated with an interface, use the **gvrpregistration**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 **gvrpregistration** command is only operational if GVRP is configured on an interface.

The **nogvrpregistration** 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.

Command	Description
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 leve.
show gvrp interface	Displays details of the adininstrative 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 **gvrptimer**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 **nogvrptimer** 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 globallly 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 adininstrative 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 **gvrpvlancreate**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-moduleslot** 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-moduleslot** command does not have a **no** form.

To start, stop, or reload a SPA, use the **hw-modulesubslot**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-moduleslot***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 **showloggingonboardslot** privileged EXEC and diagnostic mode commands.

Enter the **showloggingonboardslot***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-moduleslot***slot***loggingonboarddisable** 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 **clearloggingonboardslot** command.

When the **hw-moduleslot** 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 **showloggingonboardslotr0status**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.

Command	Description
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 internal spanning tree (CIST) instance, 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.

Command Default

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.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

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:

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

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

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

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

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

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

```
Device(config-mst)# no instance 2
Device(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.

l2protocol forward

To process or forward layer 2 Bridge Protocol Data Units (BPDU), use the **l2protocol forward** command in the interface configuration mode. To disable the command, use the **no** form of this command.

l2protocol forward [*protocol*]
no l2protocol forward

Syntax Description

protocol	Specifies the protocol which will be forwarded.

Command Default

Command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on Cisco ASR 901Series Aggregation Service Routers.

Usage Guidelines

This command is supported on the switchport main interface, layer 3 port main interface, Ethernet Virtual Circuits (EVCs), and on UNI-C and UNI-S ports. Ingress BPDUs that are processed by a service instance with l2protocol-forward configured, are treated as normal data locally on the same box, but they are sent as BPDUs on any egress trunk interfaces, outside the box.

Examples

This example shows how to process and forward layer 2 BPDUs:

```
Router(config-if)# l2protocol forward vtp
```