Transparent Layer 2 Protocol Tunneling and PDU Filtering

Layer 2 protocol tunneling allows service providers to carry traffic from multiple customers across a core network, and maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. The Transparent Layer 2 Protocol Tunneling feature allows Layer 2 protocol data units (PDUs) to be tunneled across the core network without being interpreted and processed by intermediary network devices. Layer 2 PDU filtering allows a service provider to specify which Layer 2 PDUs are to be dropped at an ingress interface on a provider edge (PE) router. Transparent Layer 2 Protocol Tunneling and PDU Filtering provide an enhanced feature set for service providers that transmit customer VLAN traffic from metro Ethernet VPNs across an MPLS core network.

Feature History for Transparent Layer 2 Protocol Tunneling and PDU Filtering

Release	Modification
12.0(28)S	This feature was introduced on 4-Port Gigabit Ethernet ISE line cards on the Cisco 12000 Series Internet Router.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Transparent Layer 2 Protocol Tunneling and PDU Filtering

- Transparent Layer 2 protocol tunneling and PDU filtering are intended for use on provider edge (PE) routers in an MPLS-enabled service-provider core network.
- Transparent Layer 2 protocol tunneling and PDU filtering are supported on main Ethernet interfaces, 802.1Q (VLAN) subinterfaces, and stacked VLAN (802.1Q-in-Q) subinterfaces on which Layer 2 Ethernet over MPLS (EoMPLS) is enabled using the **xconnect** *peer-ip-address vcid* **encapsulation mpls** command, as shown in "Configuring Transparent Layer 2 Protocol Tunneling and PDU Filtering" section on page 5.

Note The **xconnect encapsulation mpls** command replaces the deprecated **mpls l2transport route** command used to configure EoMPLS.

Use the **xconnect** *peer-ip-address vcid* **encapsulation mpls** command to bind an 802.1Q VLAN attachment circuit to an Any Transport over MPLS (AToM) pseudowire for EoMPLS. For information about how to configure and use Layer 2 tunneling on the Cisco 12000 Series Internet Router, refer to *Any Transport over MPLS*.

EoMPLS transports Layer 2 Ethernet frames across an MPLS backbone, using a point-to-point virtual circuit (VC) between PE routers. Only the PE routers at the ingress and egress points of the MPLS core network know about the VC dedicated to transporting Layer 2 traffic between customer sites.

Restrictions for Transparent Layer 2 Protocol Tunneling and PDU Filtering

- You cannot configure both transparent Layer 2 protocol tunneling and PDU filtering for a Layer 2 protocol (CDP, STP, or VTP) on the same main Ethernet interface or subinterface.

Information About Transparent Layer 2 Protocol Tunneling and PDU Filtering

To configure the Transparent Layer 2 Protocol Tunneling and PDU Filtering features, you should understand the following concepts:

- How Transparent Layer 2 Protocol Tunneling Works, page 2
- How Layer 2 PDU Filtering Works, page 4

How Transparent Layer 2 Protocol Tunneling Works

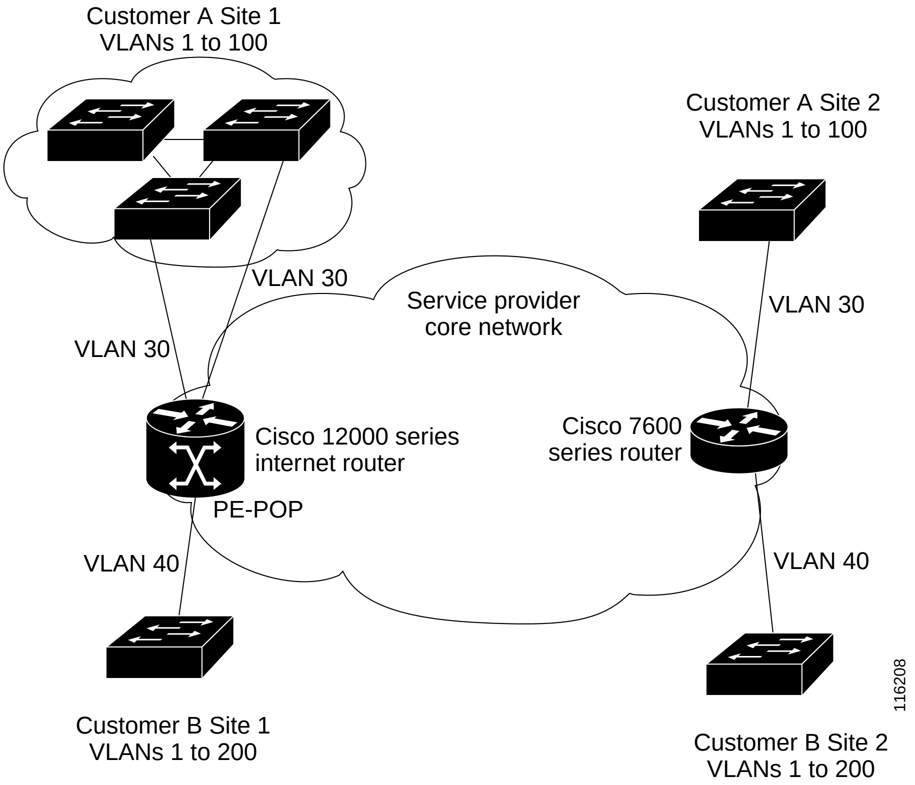
Customer VLANs at different sites connected across a service-provider network need to run various Layer 2 protocols to scale their topology to include all remote VLAN sites and local sites. For example:

- The Spanning-Tree Protocol (STP) must run properly so that each customer VLAN builds a spanning tree that includes the local site and all remote customer sites across the service-provider infrastructure.
- The Cisco Discovery Protocol (CDP) must discover neighboring Cisco devices from local and remote customer VLAN sites.
- The VLAN Trunking Protocol (VTP) must provide consistent VLAN configuration throughout all sites in a customer network.

Transparent Layer 2 protocol tunneling is performed by provider edge (PE) routers on the inbound side of the service-provider network that overwrite the customer PDU-destination MAC address in an Ethernet packet with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0). The Ethernet packet is then transparently tunneled over the core network to a peer PE router. If Layer 2 protocol tunneling is configured on the PE router on the outbound side, the destination MAC address is restored in the Layer 2 protocol information so that packets are forwarded to all ports in the same metro VLAN.

Core routers and switches in the service-provider network do not intercept and process these packets, but forward them as normal packets. Layer 2 protocol data units (PDUs) for CDP, STP, or VTP are tunneled transparently across the service-provider network and delivered to a PE router on the outbound side of the network. In Figure 1, a Cisco 12000 Series Internet Router deployed in a point of presence (PE-POP) and a Cisco 7600 series router serve as the peer PE routers.

Figure 1 Layer 2 Protocol Tunneling: Example



As shown in Figure 1, Customer A has four switches in the same VLAN that are connected through the service-provider network. A Cisco 12000 Series Internet Router and a Cisco 7600 series router serve as the PE routers that encapsulate Layer 2 protocol packets with a well-known MAC address on the inbound side of the service-provider network.

PE Ethernet subinterfaces are connected to customer 802.1Q ports. The Cisco 12000 Series Internet Router supports transparent Layer 2 protocol tunneling for CDP, STP, and VTP. The PE routers connected to customer switches perform the tunneling process.

With normal Layer 2 tunneling, identical packets are received by all PE router interfaces connected to the same customer VLAN with the following results:

- Devices on each of a customer's sites are able to properly run STP and each customer VLAN can build a correct spanning tree based on parameters from all sites and not just from the local site.
- CDP discovers and shows information about the other Cisco devices connected through the service-provider network.
- VTP provides consistent VLAN configuration throughout the customer network, propagating through the service provider to all switches.

For transparent Layer 2 protocol tunneling to occur, Layer 2 EoMPLS must be configured on the ingress and egress Ethernet main interfaces or subinterfaces of the PE routers. If the routers are not configured to tunnel Layer 2 PDUs, the peer PE router on the far end of the network cannot properly run the STP, CDP, and VTP protocols. For example, STP for a VLAN on a switch in Customer A, Site 1 will build a spanning tree on the switches at that site without considering convergence parameters based on Customer A's switch in Site 2.

You enable transparent Layer 2 tunneling by protocol (STP, CDP, or VTP) on the Ethernet interface (or subinterface) connected to a customer VLAN. Also, you can specify the MPLS EXP bits to be used for transparently tunneling Layer 2 PDUs.

You can enable transparent Layer 2 protocol tunneling on:

- A main Ethernet interface
- An 802.1Q VLAN subinterface
- An Ethernet subinterface configured for stacked VLAN (802.1Q-in-Q) processing. For more information about how to configure and use stacked VLAN processing, refer to *Stacked VLAN Processing*.

In each case, the encapsulation and de-encapsulation of the MAC address performed on Layer 2 protocol packets is the same.

How Layer 2 PDU Filtering Works

When transparent Layer 2 protocol tunneling is configured and Layer 2 PDUs that enter the inbound PE router through the tunnel exit the router into the service-provider MPLS network, the router overwrites the customer PDU-destination MAC address with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0). The PE router on the outbound side restores the Layer 2 protocol and MAC address information and forwards the packets to all ports in the same metro VLAN. Therefore, the Layer 2 PDUs are kept intact and are transparently delivered across the service-provider network to the other side of the customer network.

With Layer 2 PDU filtering, you can configure certain Layer 2 PDU frames to be dropped before they are encapsulated on the inbound PE router and transparently sent across the service-provider core network.

The Layer 2 PDU frames are identified by protocol and a well-known destination MAC address when received on an inbound PE router. By using the **l2protocol** command with the **drop** keyword, you can specify which Layer 2 PDU frames are to be dropped and not transmitted across the core MPLS network.

Configuring Transparent Layer 2 Protocol Tunneling and PDU Filtering

PREREQUISITES

- On a main Ethernet interface or subinterface, you must enable EoMPLS using the **xconnect encapsulation mpls** command.

To configure and verify transparent Layer 2 protocol tunneling and PDU filtering on a main Ethernet interface or subinterface, follow these steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*

   Or

   interface *type slot/port.subinterface-number*
4. (Optional) **encapsulation dot1q** *sp-vlan-id*

   Or

   encapsulation dot1q *sp-vlan-id* **second-dot1q** {*ce-vlan-id* | **any**}
5. **xconnect** *peer-ip-address vcid* **encapsulation mpls**
6. **l2protocol** {**cdp** | **stp** | **vtp**} [**drop** | **tunnel [experimental** *mpls-exp-value*] | **experimental** *mpls-exp-value*]
7. **end**
8. **show interfaces gigabitethernet** *slot/port* **l2protocol**

   Or

   show interfaces gigabitethernet *slot/port.subinterface-number* **l2protocol**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface`** *`type slot/port`*
	Or
	`interface` *`type slot/port.subinterface-number`*
	Example:
	`Router(config)# interface gigabitethernet 1/0.2`
		Enters interface or subinterface configuration mode to configure the Ethernet interface or subinterface.

Step 4	**`encapsulation dot1q`** *`sp-vlan-id`*
	Example:
	`Router(config-subif)# encapsulation dot1q 200`
	Or
	`encapsulation dot1q` *`sp-vlan-id`* **`second-dot1q`** `{`*`ce-vlan-id`* `|` **`any`**`}`
	Example:
	`Router(config-subif)# encapsulation dot1q 10 second-dot1q 100`
		(Optional) Use the **encapsulation dot1q** *sp-vlan-id* command only on an Ethernet subinterface to enable 802.1Q tunneling for the service-provider VLAN ID (*sp-vlan-id*) assigned to a specific customer.
		For more information about using this command to configure 802.1Q encapsulation on VLAN packets, refer to *IEEE 802.1Q-in-Q VLAN Tag Termination*.
		The **encapsulation dot1q** *sp-vlan-id* **second-dot1q** ce-*vlan-id* command enables a subinterface to process stacked VLAN (802.1Q-in-Q) Ethernet packets with the unique service-provider VLAN ID (*sp-vlan-id*) for the customer and the specified customer VLAN ID (*ce-vlan-id*) in their headers.
		- The range of valid CE-VLAN IDs is from 1 to 4095.
		- Use the **any** keyword to enable stacked VLAN processing on packets with customer VLAN IDs not specified in a separate **encapsulation dot1q** *sp-vlan-id* **second-dot1q** *ce-vlan-id* command on other subinterfaces under the same main Ethernet interface.
		For more information about how to use this command to configure stacked VLAN (802.1Q-in-Q) processing, refer to *Stacked VLAN Processing*.
		- In the first example, a subinterface is configured for 802.1Q tunneling of packets with SP-VLAN ID 200.
		- In the second example, a subinterface is configured for stacked VLAN tunneling of packets with SP-VLAN ID 10 and CE-VLAN ID 100.

	Command or Action	Purpose
Step 5	**xconnect** *peer-ip-address vcid* **encapsulation mpls** **Example:** `Router(config-subif)# xconnect 192.16.0.1 50 encapsulation mpls`	On a main Ethernet interface or subinterface, configures EoMPLS by binding an 802.1Q VLAN attachment circuit to a virtual circuit (VC) in an AToM pseudowire. The *peer-ip-address* argument specifies the IP address of the peer PE router. The *vc-id* argument is the 32-bit value that identifies the virtual circuit between the peer PE routers at each endpoint of the VC. You must configure the same VC ID on the peer PE router. For more information about how to configure EoMPLS, refer to *Any Transport over MPLS*.

Step 6	**l2protocol** {**cdp** | **stp** | **vtp**} {**tunnel** [**experimental** *mpls-exp-value*] | **experimental** *mpls-exp-value*}
	Example:
	`Router(config-subif)# l2protocol cdp tunnel experimental 7`
		Configures transparent Layer 2 protocol tunneling on the interface or subinterface for a specified Layer 2 protocol (CDP, STP, or VTP).
		• To transparently tunnel the specified Layer 2 PDU frames after changing the MAC destination address, enter the **tunnel** keyword.
		• To transparently tunnel the specified Layer 2 PDU frames after changing the MAC destination address and rewriting the experimental (EXP) field bit in MPLS labels, enter **tunnel experimental** *mpls-exp-value*, where *mpls-exp-value* is a value from 0 to 7.
		• To transparently tunnel the specified Layer 2 PDU frames in MPLS packets using EoMPLS (without transparent Layer 2 protocol tunneling) and rewrite the specified experimental (EXP) field bit in MPLS labels, enter **experimental** *mpls-exp-value*, where *mpls-exp-value* is from 0 to 7.
		• In the example, all Ethernet VLAN packets with Layer 2 CDP headers are transparently tunneled after the EXP field is changed to 7.

Step 7	**l2protocol** {**cdp** | **stp** | **vtp**} **drop** **Example:** `Router(config-subif)# l2protocol stp drop`	Configures the specified Layer 2 PDU frames to be dropped and not transmitted across the core MPLS network. • In the example, all Ethernet VLAN packets with Layer 2 STP headers are filtered out and not transmitted.

	Command or Action	Purpose

Step 8	**end**
	Example:
	`Router(config-subif)# end`
		Exits interface or subinterface configuration mode and returns to privileged EXEC mode.

Step 9	**show interfaces gigabitethernet** *slot/port* **l2protocol** Or **show interfaces gigabitethernet** *slot/port.subinterface-number* **l2protocol** **Example:** `Router# show interfaces gigabitethernet 1/0.2 l2protcol`	(Optional) Verifies the transparent Layer 2 protocol tunneling and PDU filtering configuration on a specified Gigabit Ethernet interface or subinterface.

Configuration Examples for Transparent Layer 2 Protocol Tunneling and PDU Filtering

This section provides the following configuration examples:

- Configuring Transparent Layer 2 Protocol Tunneling and PDU Filtering: Example, page 8
- Displaying Transparent Layer 2 Protocol Tunneling and PDU Filtering Statistics: Example, page 9

Configuring Transparent Layer 2 Protocol Tunneling and PDU Filtering: Example

The following example shows how to configure a Gigabit Ethernet subinterface on a Cisco 12000 Series Internet Router used as a PE router in a service-provider MPLS core network so that PDUs from Layer 2:

- Cisco Discovery Protocol (CDP) are filtered out.
- Spanning Tree Protocol (STP) are transmitted using normal Layer 2 protocol tunneling and changing the MPLS experimental bit to 4.
- VLAN Trunking Protocol (VTP) are tunneled by assigning a well-known Cisco proprietary MAC address and changing the MPLS experimental bit to 0.

Note that this configuration example is valid for an Ethernet subinterface configured for 802.1Q VLAN tunneling.

Prerequisites

- You must enable EoMPLS on an Ethernet subinterface using the **xconnect encapsulation mpls** command.

```
Router# enable
Router# configure terminal
Router(config)# interface gigabitethernet 3/0.5
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# xconnect 7.7.7.7 70 encapsulation mpls
Router(config-subif)# l2protocol cdp drop
Router(config-subif)# l2protocol stp experimental 4
Router(config-subif)# l2protocol vtp tunnel experimental 0
Router(config-subif)# end
```

Displaying Transparent Layer 2 Protocol Tunneling and PDU Filtering Statistics: Example

The following example shows how to display statistical information about the Layer 2 protocols that are tunneled and dropped on a Gigabit Ethernet subinterface at one end of a Layer 2 protocol tunnel:

```
Router# show interfaces gigabitethernet 3/0.5 l2protocol
GigabitEthernet3/0.5
Protocol     Pkts In     Chars In    Pkts Out     Chars Out
cdp          1000        64000       0            0
stp          1000        64000       0            0
vtp          1000        64000       0            0
```

Additional References

The following sections provide references related to the Transparent Layer 2 Protocol Tunneling and PDU Filtering feature:

Related Documents

Related Topic	Document Title
Interface commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Switching Services Configuration Guide*, Release 12.3 *Cisco IOS Switching Services Command Reference*, Release 12.3
Description of software functionality and commands supported on the 4-Port Gigabit Ethernet ISE line card	*4-Port Gigabit Ethernet ISE Line Card for Cisco 12000 Series Internet Router*
Description of VLANs based on 802.1Q and 802.1Q-in-Q	*Cisco Metro Ethernet Access Services*
VLAN routing	*Routing Between Virtual LANs Overview*
Procedure for configuring EoMPLS	*Any Transport over MPLS*
Procedure for configuring VLANs for routing using 802.1Q VLAN encapsulation	"Configuring 802.1Q VLAN Encapsulation" section in *Configuring Virtual LAN Encapsulation*
Procedure for configuring support for double-tagged 802.1Q-in-Q VLANs on Cisco 75000 Series Ethernet subinterfaces	*IEEE 802.1Q-in-Q VLAN Tag Termination*
Procedure for configuring support for double-tagged, stacked VLAN (802.1Q-in-Q) processing on Cisco 12000 Series Ethernet subinterfaces	*Stacked VLAN Processing*

Standards

Standards	Title
IEEE 802.1Q	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- l2protocol
- show interfaces gigabitethernet l2protocol

l2protocol

To configure transparent protocol tunneling and PDU filtering for Layer 2 control packets transmitted over an MPLS service-provider network, use the **l2protocol** command in interface or subinterface configuration mode.

l2protocol {**cdp** | **stp** | **vtp**} {**drop** | **tunnel experimental** *mpls-exp-id* | **experimental** *mpls-exp-id***}**

no l2protocol {**cdp** | **stp** | **vtp**} {**drop** | **tunnel experimental** *mpls-exp-id* | **experimental** *mpls-exp-id***}**

Syntax Description

cdp	Configures transparent Layer 2 protocol tunneling or PDU filtering for Ethernet VLAN frames that contain Cisco Discovery Protocol (CDP) packets.
stp	Configures transparent Layer 2 protocol tunneling or PDU filtering for Ethernet VLAN frames that contain Spanning Tree Protocol (STP) packets.
vtp	Configures transparent Layer 2 protocol tunneling or PDU filtering for Ethernet VLAN frames that contain VLAN Trunk Protocol (VTP) packets.
drop	Configures PDU filtering to drop Ethernet VLAN frames that contain the specified Layer 2 protocol (CDP, STP, or VTP) packet.
tunnel	Configures transparent Layer 2 protocol tunneling to transmit Ethernet VLAN frames that contain the specified Layer 2 protocol (CDP, STP, or VTP) packet.
tunnel experimental *mpls-exp-id*	Configures transparent Layer 2 protocol tunneling to transmit Ethernet VLAN frames that contain the specified Layer 2 protocol (CDP, STP, or VTP) packet by imposing the specified *mpls-exp-id* value in the MPLS experimental field. Valid values are from 0 to 7.
experimental *mpls-exp-id*	Configures normal 802.1Q or stacked VLAN (802.1Q-in-Q) tunneling (without transparent Layer 2 protocol tunneling) to transmit Ethernet VLAN frames that contain the specified Layer 2 protocol (CDP, STP, or VTP) packet by imposing the specified *mpls-exp-id* value in the MPLS experimental field. Valid values are from 0 to 7.

Defaults

This command has no default settings.

Command Modes

Interface configuration or subinterface configuration

Command History

Release	Modification
12.0(28)S	This command was introduced on Cisco 12000 Series 4-Port Gigabit Ethernet ISE line cards.

Usage Guidelines

Layer 2 protocol tunneling allows Layer 2 protocol data units (PDUs) to be tunneled transparently through a service-provider network. Layer 2 PDUs, such as CDP, STP, and VTP, are transmitted between peer PE routers without being interpreted and processed by intermediary network devices.

Transparent Layer 2 protocol tunneling is performed by PE routers on the inbound side of the service-provider network that overwrite the customer PDU-destination MAC address in an Ethernet packet with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0). Ethernet packets are transparently tunneled over the core network to a peer PE router. The PE router on the outbound side restores the Layer 2 protocol and MAC address information and forwards the packets to all ports in the same metro VLAN.

Layer 2 PDU filtering allows a service provider to specify which Layer 2 PDUs are to be dropped at an ingress interface on a PE router. The specified Layer 2 PDU frames are not transmitted over the core network, and are filtered before they are encapsulated for transparent Layer 2 protocol tunneling.

Use the **l2protocol** command to configure transparent Layer 2 protocol tunneling or PDU filtering on an Ethernet interface or subinterface in a PE router in an MPLS-enabled service-provider network.

The following prerequisite applies for configuring transparent Layer 2 protocol tunneling and PDU filtering:

- On a main Ethernet interface or subinterface, you must configure EoMPLS (using the **xconnect encapsulation mpls** command).

Although 802.1Q VLAN and stacked VLAN tunneling are not required for transparent Layer 2 protocol tunneling and/or PDU filtering, you can configure these features as follows:

- On a main Ethernet interface, you enable 802.1Q tunneling using the **encapsulation dot1q** command.
- On an Ethernet subinterface, you enable 802.1Q tunneling using the **encapsulation dot1q** command or stacked VLAN (802.1Q-in-Q) tunneling using the **encapsulation dot1q second-dot1q** command.

To verify a Layer 2 protocol tunneling or PDU filtering configuration on a Gigabit Ethernet interface or subinterface, use the **show interfaces gigabitethernet l2protocol** command.

Examples

The following example shows how to configure a Gigabit Ethernet subinterface on a Cisco 12000 Series Internet Router used as a PE router in a service-provider MPLS core network so that PDUs from Layer 2:

- Cisco Discovery Protocol (CDP) frames are transmitted (without transparent Layer 2 tunneling) by changing the MPLS experimental bit to 5.
- Spanning Tree Protocol (STP) frames are filtered out at the ingress PE router.
- VLAN Trunking Protocol (VTP) frames are transparently tunneled by assigning a well-known Cisco proprietary MAC address and changing the MPLS experimental bit to 0.

Note that this configuration example applies to a Gigabit Ethernet subinterface configured for stacked VLAN 802.1Q-in-Q tunneling and EoMPLS to a destination address 7.7.7.7 on VC 70.

```
Router# enable
Router# configure terminal
Router(config)# interface gigabitethernet 3/0.5
Router(config-subif)# encapsulation dot1q 20 second-dot1q 3
Router(config-subif)# xconnect 7.7.7.7 70 encapsulation mpls
Router(config-subif)# l2protocol cdp experimental 5
Router(config-subif)# l2protocol stp drop
Router(config-subif)# l2protocol vtp tunnel experimental 0
Router(config-subif)# end
```

Related Commands

Command	Description
show interfaces gigabitethernet l2protocol	Displays statistical information about Layer 2 protocol tunneling and PDU filtering on a main Gigabit Ethernet interface or subinterface.

show interfaces gigabitethernet l2protocol

To display statistical information about Layer 2 protocol tunneling and PDU filtering configured on a specified Gigabit Ethernet interface or subinterface, use the **show interfaces gigabitethernet l2protocol** command in privileged EXEC mode.

show interfaces gigabitethernet {*slot/port* | *slot/port.subinterface-number*} **l2protocol**

Syntax Description

slot/port	Slot and port numbers of a main Gigabit Ethernet interface.
slot/port.subinterface-number	Slot, port, and subinterface numbers of a Gigabit Ethernet subinterface.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(28)S	This command was introduced on Cisco 12000 Series 4-Port Gigabit Ethernet ISE line cards.

Usage Guidelines

Use the **show interfaces gigabitethernet l2transport** command to display statistics for Layer 2 protocol tunneling and PDU filtering configured on a Gigabit Ethernet interface or subinterface on a PE router in an MPLS service-provider network.

Examples

The following example shows how to display statistical information about Layer 2 protocol tunneling and PDU filtering configured on a Gigabit Ethernet subinterface:

```
Router# show interfaces gigabitethernet 2/0.1 l2protocol

GigabitEthernet2/0.1
Protocol   Pkts In    Chars In   Pkts Out   Chars Out
cdp        0          0          1000       38000
stp        0          0          1000       38000
vtp        0          0          1000       38000
```

Table 1 describes the significant fields shown in the display.

Table 1 show interfaces gigabitethernet l2protocol Field Descriptions

Field	Description
Protocol	Layer 2 protocol data unit (PDU)
Pkts In	Number of packets received
Chars In	Number of bytes received

Table 1 show interfaces gigabitethernet l2protocol Field Descriptions (continued)

Field	Description
Pkts Out	Number of packets transmitted
Chars Out	Number of bytes transmitted

Related Commands

Command	Description
l2protocol	Configures Layer 2 protocol tunneling and PDU filtering for Layer 2 control packets transmitted over an MPLS service-provider network.

Glossary

802.1Q—IEEE 802.1Q protocol used to interconnect multiple switches and routers, and for defining VLAN topologies.

802.1Q-in-Q—Support for double-tagged VLAN Ethernet packets in which an 802.1Q tag from a customer VLAN (called CE-VLAN ID) is encapsulated in a second 802.1Q tag from a service-provider network (called an SP-VLAN ID).

Bridge protocol data unit (BPDU)—Spanning-Tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network. See also **PDU**.

CDP—Cisco Discovery Protocol. CDP is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to display information about the interfaces a router uses.

CE router—Customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

CE-VLAN—Customer edge VLAN. 802.1Q tag used in packets received from customer VLANs that enter a service-provider network. In stacked VLAN (802.1Q-in-Q) processing, all customer VLAN IDs are encapsulated in a service-provider VLAN ID assigned to the customer. Also known as the “inner” VLAN ID in 802.1Q-in-Q encapsulation. See also **SP-VLAN**.

encapsulation—Wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. See also **tunneling**.

EoMPLS—Ethernet over Multiprotocol Label Switching (MPLS). A tunneling mechanism that allows a service provider to tunnel customer Layer 2 traffic though a Layer 3 MPLS network. EoMPLS is a point-to-point solution only. EoMPLS is also known Layer 2 tunneling.

frame—Logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and trailer, used for synchronization and error control, that surround the user data contained in the unit.

ISE—IP Services Engine. ISE line cards for Cisco 12000 Series Internet Routers provide enhanced Layer 3 capabilities for high-speed customer aggregation, backbone connectivity, and peering solutions. These line cards are available in both concatenated and channelized versions.

Layer 2 Tunnel Protocol (L2TP)—An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F and PPTP, L2TP provides an industry-wide interoperable method of implementing VPDN.

Layer 3 Switching—An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F and PPTP, L2TP provides an industry-wide interoperable method of implementing VPDN.

MIB—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MPLS—Multiprotocol Label Switching. MPLS forwards IP traffic using a label. This label instructs the routers and switches in the network where to forward the packets based on pre-established IP routing information.

packet—Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data.

PDU—Protocol data unit. OSI term for packet.

PE router—Provider edge router. A router that is part of a service provider's network and is connected to a customer edge (CE) router.

POP—Point of presence. In an Operations Support System (OSS), a physical location where an interexchange carrier installed equipment to interconnect with a local exchange carrier (LEC).

SP-VLAN—Service-provider VLAN. A second layer of 802.1Q tag added to the 802.1Q-tagged packets that enter a service-provider network. This is a unique VLAN ID assigned by a service provider to encapsulate all VLAN IDs from a given customer. Also known as the “outer” VLAN ID in 802.1Q-in-Q encapsulation. See also **CE-VLAN**.

STP—Spanning Tree Protocol. STP is a broadcast algorithm used by network bridge connections to dynamically discover a loop-free subset of the network topology while maintaining a path between every pair of LANs or VLANs in the network.

tunneling—Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. See also **encapsulation**.

VLAN—Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VPN— Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunnels to encrypt all information at the IP level.

VTP—VLAN Trunk Protocol. VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. With VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network.

Note Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.