



# Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling

With Release 12.1(13)E and later, the Catalyst 6500 series switches support IEEE 802.1Q tunneling and Layer 2 protocol tunneling. This chapter describes how to configure IEEE 802.1Q tunneling and Layer 2 protocol tunneling on the Catalyst 6500 series switches.



## Note

- For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.
- The WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6148-GE-TX, and WS-X6148V-GE-TX switching modules do not support IEEE 802.1Q tunneling or Layer 2 protocol tunneling.

This chapter consists of these sections:

- [Understanding How 802.1Q Tunneling Works](#), page 14-1
- [802.1Q Tunneling Configuration Guidelines and Restrictions](#), page 14-4
- [Configuring 802.1Q Tunneling](#), page 14-5
- [Understanding How Layer 2 Protocol Tunneling Works](#), page 14-7
- [Configuring Support for Layer 2 Protocol Tunneling](#), page 14-8

## Understanding How 802.1Q Tunneling Works

802.1Q tunneling enables 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.

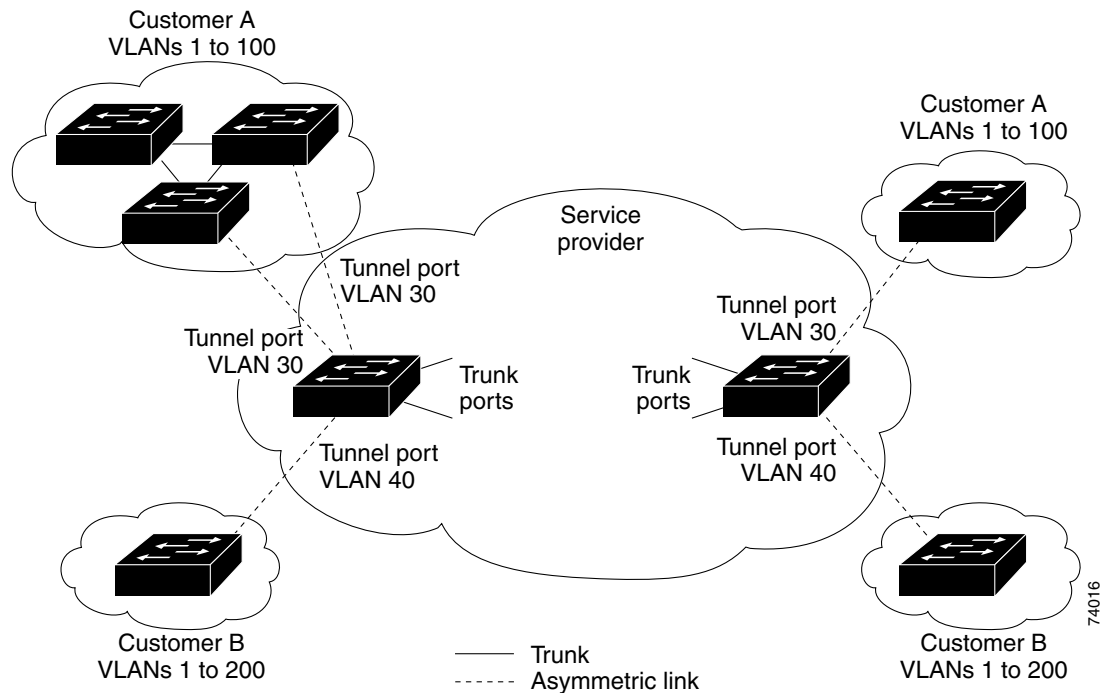
A port configured to support 802.1Q tunneling is called a tunnel port. When you configure tunneling, you assign a tunnel port to a VLAN that you dedicate to tunneling, which then becomes a tunnel VLAN. To keep customer traffic segregated, each customer requires a separate tunnel VLAN, but that one tunnel VLAN supports all of the customer's VLANs.

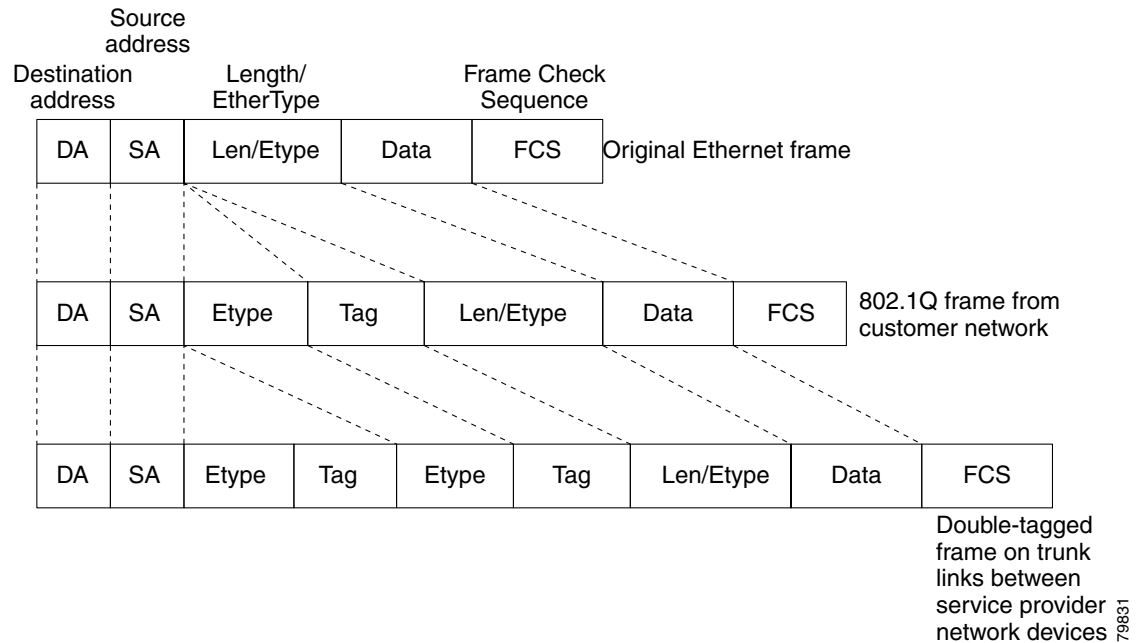
802.1Q tunneling is not restricted to point-to-point tunnel configurations. Any tunnel port in a tunnel VLAN is a tunnel entry and exit point. An 802.1Q tunnel can have as many tunnel ports as are needed to connect customer switches.

The customer switches are trunk connected, but with 802.1Q tunneling, the service provider switches only use one service provider VLAN to carry all the customer VLANs, instead of directly carrying all the customer VLANs.

With 802.1Q tunneling, tagged customer traffic comes from an 802.1Q trunk port on a customer device and enters the service-provider edge switch through a tunnel port. The link between the 802.1Q trunk port on a customer device and the tunnel port is called an asymmetrical link because one end is configured as an 802.1Q trunk port and the other end is configured as a tunnel port. You assign the tunnel port to an access VLAN ID unique to each customer. See [Figure 14-1 on page 14-2](#) and [Figure 14-2 on page 14-3](#).

**Figure 14-1 IEEE 802.1Q Tunnel Ports in a Service-Provider Network**



**Figure 14-2 Untagged, 802.1Q-Tagged, and Double-Tagged Ethernet Frames**

When a tunnel port receives tagged customer traffic from an 802.1Q trunk port, it does not strip the received 802.1Q tag from the frame header; instead, the tunnel port leaves the 802.1Q tag intact, adds a 2-byte Ethertype field (0x8100) followed by a 2-byte field containing the priority (CoS) and the VLAN. The received customer traffic is then put into the VLAN to which the tunnel port is assigned. This Ethertype 0x8100 traffic, with the received 802.1Q tag intact, is called tunnel traffic.

A VLAN carrying tunnel traffic is an 802.1Q tunnel. The tunnel ports in the VLAN are the tunnel's ingress and egress points.

The tunnel ports do not have to be on the same network device. The tunnel can cross other network links and other network devices before reaching the egress tunnel port. A tunnel can have as many tunnel ports as required to support the customer devices that need to communicate through the tunnel.

An egress tunnel port strips the 2-byte Ethertype field (0x8100) and the 2-byte length field and transmits the traffic with the 802.1Q tag still intact to an 802.1Q trunk port on a customer device. The 802.1Q trunk port on the customer device strips the 802.1Q tag and puts the traffic into the appropriate customer VLAN.

**Note**

Tunnel traffic carries a second 802.1Q tag only when it is on a trunk link between service-provider network devices, with the outer tag containing the service-provider-assigned VLAN ID and the inner tag containing the customer-assigned VLAN IDs.

# 802.1Q Tunneling Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring 802.1Q tunneling in your network:

## Restrictions

- Because tunnel traffic has the added ethertype and length field and retains the 802.1Q tag within the switch, the following restrictions exist:
  - The Layer 3 packet within the Layer 2 frame cannot be identified in tunnel traffic.
  - Layer 3 and higher parameters cannot be identified in tunnel traffic (for example, Layer 3 destination and source addresses).
  - Because the Layer 3 addresses cannot be identified within the packet, tunnel traffic cannot be routed.
  - The switch can provide only MAC-layer filtering for tunnel traffic (VLAN IDs and source and destination MAC addresses).
  - The switch can provide only MAC-layer access control and QoS for tunnel traffic.
  - QoS cannot detect the received CoS value in the 802.1Q 2-byte Tag Control Information field.
- Tunnel ports learn customer MAC addresses.
- On an asymmetrical link, the Cisco Discovery Protocol (CDP) reports a native VLAN mismatch if the VLAN of the tunnel port does not match the native VLAN of the 802.1Q trunk. The 802.1Q tunnel feature does not require that the VLANs match. Ignore the messages if your configuration requires nonmatching VLANs.
- Asymmetrical links do not support the Dynamic Trunking Protocol (DTP), because only one port on the link is a trunk. Configure the 802.1Q trunk port on an asymmetrical link to trunk unconditionally.
- Jumbo frames can be tunneled as long as the jumbo frame length combined with the 802.1Q tag does not exceed the maximum frame size.
- The 802.1Q tunneling feature cannot be configured on ports configured to support private VLANs
- VLAN Trunk Protocol (VTP) does not work between the following devices:
  - Devices connected by an asymmetrical link
  - Devices communicating through a tunnel



**Note** VTP works between tunneled devices if Layer 2 protocol tunneling is enabled. See the [“Configuring Support for Layer 2 Protocol Tunneling”](#) section on page 14-8 for configuration details.

## Guidelines

- Use asymmetrical links to put traffic into a tunnel or to remove traffic from a tunnel.
- Configure tunnel ports only to form an asymmetrical link.
- Dedicate one VLAN for each tunnel.
- Assign only tunnel ports to VLANs used for tunneling.

- Trunks require no special configuration to carry tunnel VLANs.
- We recommend that you use ISL trunks to carry tunnel traffic between devices that do not have tunnel ports. Because of the 802.1Q native VLAN feature, using 802.1Q trunks requires that you be very careful when you configure tunneling: a mistake might direct tunnel traffic to a non-tunnel port.
- Ensure that the native VLAN of the 802.1Q trunk port in an asymmetrical link carries no traffic. Because traffic in the native VLAN is untagged, it cannot be tunneled correctly. Alternatively, you can enter the global **vlan dot1q tag native** command to tag native VLAN egress traffic and drop untagged native VLAN ingress traffic.
- The following Layer 2 protocols work between devices connected by an asymmetrical link:
  - CDP
  - UniDirectional Link Detection (UDLD)
  - Port Aggregation Protocol (PAgP)
  - Link Aggregation Control Protocol (LACP)
- With Release 12.1(13)E and later releases, PortFast BPDU filtering is enabled automatically on tunnel ports. With releases earlier than Release 12.1(13)E, you can manually enable PortFast BPDU filtering on tunnel ports (see the “[Enabling PortFast BPDU Filtering](#)” section on page 16-10).
- With Release 12.1(13)E and later releases, CDP is automatically disabled on tunnel ports. With releases earlier than Release 12.1(13)E, you can manually disable CDP when you enable 802.1Q tunneling (see the “[Enabling CDP on a Port](#)” section on page 30-2).
- To configure an EtherChannel as an asymmetrical link, all ports in the EtherChannel must have the same tunneling configuration. Because the Layer 3 packet within the Layer 2 frame cannot be identified, you must configure the EtherChannel to use MAC-address-based frame distribution.
- Because all the BPDUs are being dropped, spanning tree PortFast can be enabled on Layer 2 protocol tunnel ports as follows:

```
Router(config-if)# spanning-tree portfast trunk
```

- If the service provider does not want the customer to see its switches, CDP should be disabled on the 802.1Q tunnel port as follows:

```
Router(config-if)# no cdp enable
```

## Configuring 802.1Q Tunneling

These sections describe 802.1Q tunneling configuration:

- [Preconfiguration Tasks, page 14-6](#)
- [Configuring 802.1Q Tunnel Ports, page 14-6](#)
- [Configuring the Switch to Tag Native VLAN Traffic, page 14-7](#)



### Caution

Ensure that only the appropriate tunnel ports are in any VLAN used for tunneling and that one VLAN is used for each tunnel. Incorrect assignment of tunnel ports to VLANs can forward traffic inappropriately.

## Preconfiguration Tasks

Before you can configure Layer 2 protocol tunneling, you must perform these tasks:

- Step 1** On all the service provider edge switches, PortFast BPDU filtering must be enabled on the 802.1Q tunnel ports as follows:

```
Router(config-if)# spanning-tree bpdupfilter enable
Router(config-if)# spanning-tree portfast
```



**Note** With Release 12.1(13)E and later releases, PortFast BPDU filtering is enabled automatically on tunnel ports. With releases earlier than Release 12.1(13)E, you must manually enable PortFast BPDU filtering on tunnel ports.

- Step 2** At least one VLAN must be available for Native VLAN tagging (**vlan dot1q tag native** option). If you use all the available VLANs and then try to enable the **vlan dot1q tag native** option, the option will not be enabled.

- Step 3** On all the service provider core switches, tag native VLAN egress traffic and drop untagged native VLAN ingress traffic by entering the following command:

```
Router(config)# vlan dot1q tag native
```

- Step 4** On all the customer switches, *either* enable or disable the global **vlan dot1q tag native** option.



**Note** If this option is enabled on one switch and disabled on another switch, all traffic is dropped; all customer switches must have this option configured the same on each switch.

## Configuring 802.1Q Tunnel Ports

To configure 802.1Q tunneling on a port, perform this task:

	Command	Purpose
<b>Step 1</b>	Router(config)# <b>interface</b> <i>type</i> <sup>1</sup> <i>slot/port</i>	Selects the LAN port to configure.
<b>Step 2</b>	Router(config-if)# <b>switchport</b>	Configures the LAN port for Layer 2 switching: <ul style="list-style-type: none"> <li>You must enter the <b>switchport</b> command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional <b>switchport</b> commands with keywords.</li> <li>Required only if you have not entered the <b>switchport</b> command already for the interface.</li> </ul>
<b>Step 3</b>	Router(config-if)# <b>switchport mode dot1qtunnel</b>	Configures the Layer 2 port as a tunnel port.
	Router(config-if)# <b>no switchport mode dot1qtunnel</b>	Clears the tunnel port configuration.

	Command	Purpose
Step 4	Router(config-if)# <b>end</b>	Exits configuration mode.
Step 5	Router# <b>show dot1q-tunnel</b> [{interface type interface-number}]	Verifies the configuration.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to configure tunneling on port 4/1 and verify the configuration:

```
Router# configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dot1qtunnel
Router(config-if)# end
Router# show dot1q-tunnel interface
```

## Configuring the Switch to Tag Native VLAN Traffic

The `vlan dot1q tag native` command is a global command that configures the switch to tag native VLAN traffic, and admit only 802.1Q tagged frames on 802.1Q trunks, dropping any untagged traffic, including untagged traffic in the native VLAN.

To configure the switch to tag traffic in the native VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# <b>vlan dot1q tag native</b>	Configures the switch to tag native VLAN traffic.
	Router(config)# <b>no vlan dot1q tag native</b>	Clears the configuration.
Step 2	Router(config)# <b>end</b>	Exits configuration mode.
Step 3	Router# <b>show vlan dot1q tag native</b>	Verifies the configuration.

This example shows how to configure the switch to tag native VLAN traffic and verify the configuration:

```
Router# configure terminal
Router(config)# vlan dot1q tag native
Router(config)# end
Router# show vlan dot1q tag native
```

## Understanding How Layer 2 Protocol Tunneling Works

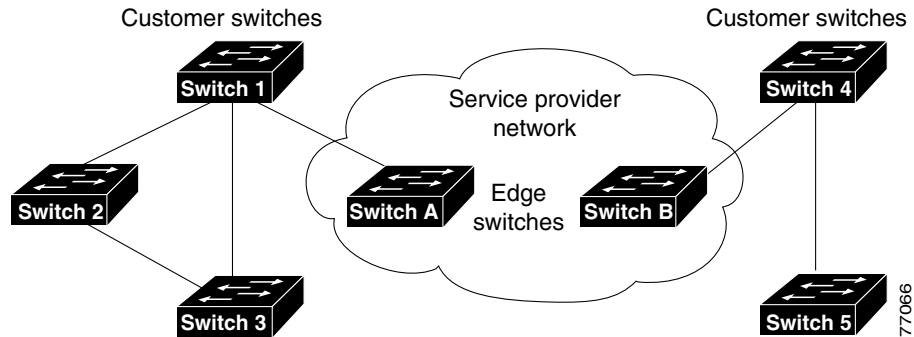
Layer 2 protocol tunneling allows Layer 2 protocol data units (PDUs) (CDP, STP, and VTP) to be tunneled through a network. This section uses the following terminology:

- Edge switch—The switch connected to the customer switch and placed on the boundary of the service provider network (see [Figure 14-3](#)).
- Layer 2 protocol tunnel port—A port on the edge switch on which a specific tunneled protocol can be encapsulated or deencapsulated. The Layer 2 protocol tunnel port is configured through CLI commands.
- Tunneled PDU—A CDP, STP, or VTP PDU.

Without Layer 2 protocol tunneling, tunnel ports drop STP and VTP packets and process CDP packets. This handling of the PDUs creates different spanning tree domains (different spanning tree roots) for the customer switches. For example, STP for a VLAN on switch 1 (see [Figure 14-3](#)) builds a spanning tree

topology on switches 1, 2, and 3 without considering convergence parameters based on switches 4 and 5. To provide a single spanning tree domain for the customer, a generic scheme to tunnel BPDUs was created for control protocol PDUs (CDP, STP, and VTP). This process is referred to as Generic Bridge PDU Tunneling (GBPT).

**Figure 14-3 Layer 2 Protocol Tunneling Network Configuration**



GBPT provides a scalable approach to PDU tunneling by software encapsulating the PDUs in the ingress edge switches and then multicasting them in hardware. All switches inside the service provider network treat these encapsulated frames as data packets and forward them to the other end. The egress edge switch listens for these special encapsulated frames and deencapsulates them; they are then forwarded out of the tunnel.

The encapsulation involves rewriting the destination media access control (MAC) address in the PDU. An ingress edge switch rewrites the destination MAC address of the PDUs received on a Layer 2 tunnel port with the Cisco proprietary multicast address (01-00-0c-cd-cd-d0). The PDU is then flooded to the native VLAN of the Layer 2 tunnel port. If you enable Layer 2 protocol tunneling on a port, PDUs of an enabled protocol are not sent out. If you disable Layer 2 protocol tunneling on a port, the disabled protocols behave the same way they were behaving before Layer 2 protocol tunneling was disabled on the port.

## Configuring Support for Layer 2 Protocol Tunneling



### Note

Encapsulated PDUs received by an 802.1Q tunnel port are transmitted from other tunnel ports in the same VLAN on the switch.

To configure Layer 2 protocol tunneling on a port, perform this task:

	Command	Purpose
Step 1	Router(config)# <b>interface</b> <i>type</i> <sup>1</sup> <i>slot/port</i>	Selects the LAN port to configure.
Step 2	Router(config-if)# <b>switchport</b>	Configures the LAN port for Layer 2 switching: <ul style="list-style-type: none"> <li>You must enter the <b>switchport</b> command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional <b>switchport</b> commands with keywords.</li> <li>Required only if you have not entered the <b>switchport</b> command already for the interface.</li> </ul>
Step 3	Router(config-if)# <b>l2protocol-tunnel</b> [ <b>cdp</b>   <b>drop-threshold</b> [ <i>packets</i> ]   <b>shutdown-threshold</b> [ <i>packets</i> ]   <b>stp</b>   <b>vtp</b> ]	Configures the Layer 2 port as a Layer 2 protocol tunnel port for the protocol(s) specified.
	Router(config-if)# <b>no l2protocol-tunnel</b> [ <b>cdp</b>   <b>drop-threshold</b>   <b>shutdown-threshold</b>   <b>stp</b>   <b>vtp</b> ]	Clears the configuration.
Step 4	Router(config)# <b>end</b>	Exits configuration mode.
Step 5	Router# <b>show l2protocol-tunnel</b> [ <b>interface</b> <i>type</i> <sup>1</sup> <i>slot/port</i>   <b>summary</b> ]	Verifies the configuration.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

When you configure a Layer 2 port as a Layer 2 protocol tunnel port, note the following syntax information:

- Optionally, you may specify a drop-threshold for the port. The drop-threshold value, from 1 to 4096, determines the number of packets to be processed for that protocol on that interface in one second. When the drop threshold is exceeded, PDUs for the specified protocol are dropped for the remainder of the 1-second period. If a shutdown threshold is not specified, the value is 0 (shutdown threshold disabled).
- Optionally, you may specify a shutdown-threshold for the port. The drop-threshold value, from 1 to 4096, determines the number of packets to be processed for that protocol on that interface in one second. When the shutdown threshold is exceeded, the port is put in errdisable state. If a shutdown threshold is not specified, the value is 0 (shutdown threshold disabled).



**Note**

A new keyword, **l2ptguard**, has been added to the following commands:

- errdisable detect cause**
- errdisable recovery cause**

Refer to the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide—Release 12.1 E* publication for more information.

This example shows how to configure Layer 2 protocol tunneling and shutdown thresholds on port 5/1 for CDP, STP, and VTP, and verify the configuration:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel shutdown-threshold cdp 10
Router(config-if)# l2protocol-tunnel shutdown-threshold stp 10
Router(config-if)# l2protocol-tunnel shutdown-threshold vtp 10
Router(config-if)# end
Router# show l2protocol-tunnel summary
Port   Protocol          Threshold
              (cos/cdp/stp/vtp)
-----
Fa5/1  cdp stp vtp      0/10 /10 /10      down trunk
Router#
```

This example shows how to display counter information for port 5/1:

```
Router# show l2protocol-tunnel interface fastethernet 5/1
Port   Protocol          Threshold          Counters
              (cos/cdp/stp/vtp) (cdp/stp/vtp/decap)
-----
Router#
```

This example shows how to clear the Layer 2 protocol tunneling configuration from port 5/1:

```
Router(config-if)# no l2protocol-tunnel shutdown-threshold cdp 10
Router(config-if)# no l2protocol-tunnel shutdown-threshold stp 10
Router(config-if)# no l2protocol-tunnel shutdown-threshold vtp 10
Router(config-if)# no l2protocol-tunnel cdp
Router(config-if)# no l2protocol-tunnel stp
Router(config-if)# no l2protocol-tunnel vtp
Router(config-if)# end
Router# show l2protocol-tunnel summary
Port   Protocol          Threshold
              (cos/cdp/stp/vtp)
-----
Router#
```

This example shows how to clear Layer 2 protocol tunneling port counters:

```
Router# clear l2protocol-tunnel counters
Router#
```