



CHAPTER 21

Configuring IEEE 802.1Q Tunneling

This chapter describes how to configure IEEE 802.1Q tunneling in Cisco IOS Release 12.2SX.



Note

- For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, Release 12.2SX, at this URL:
http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
 - 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.
-



Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

This chapter consists of these sections:

- [Understanding 802.1Q Tunneling, page 21-1](#)
- [802.1Q Tunneling Configuration Guidelines and Restrictions, page 21-3](#)
- [Configuring 802.1Q Tunneling, page 21-6](#)

Understanding 802.1Q Tunneling

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 21-1 on page 21-2](#) and [Figure 21-2 on page 21-3](#).

Figure 21-1 IEEE 802.1Q Tunnel Ports in a Service-Provider Network

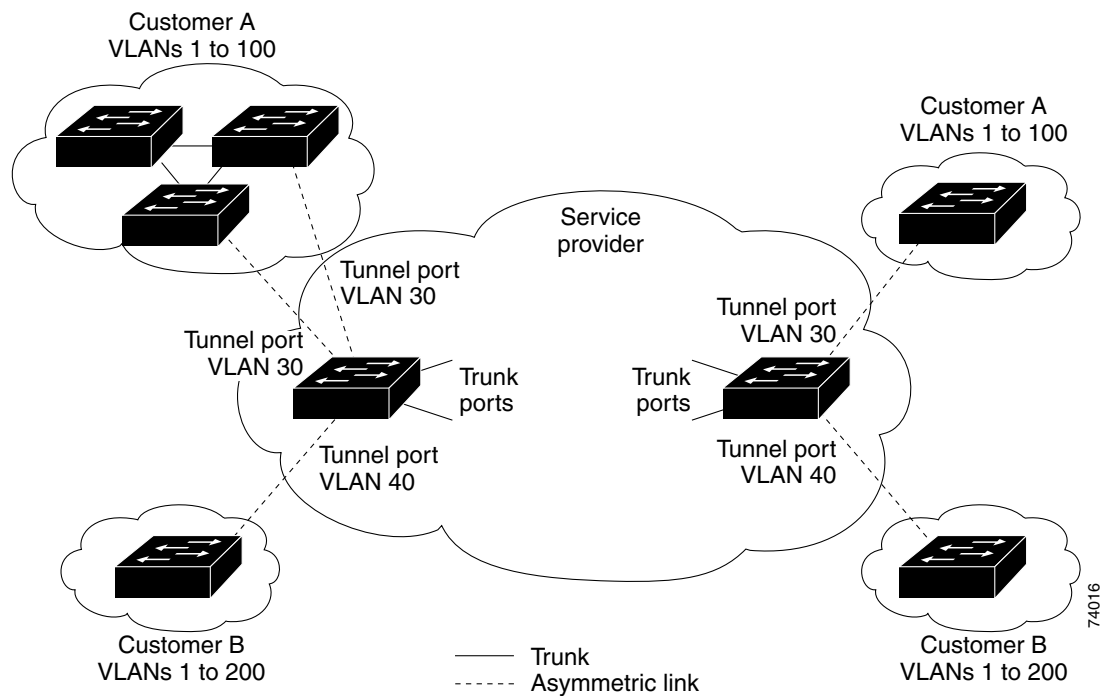
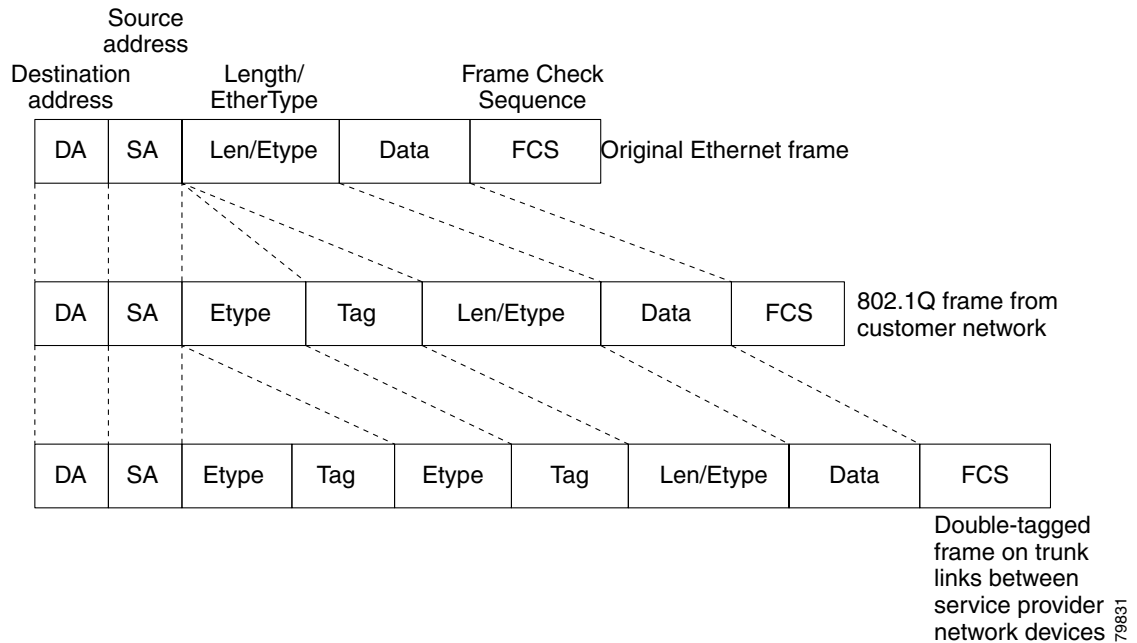


Figure 21-2 Untagged, 802.1Q-Tagged, and Double-Tagged Ethernet Frames

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

When configuring 802.1Q tunneling in your network, follow these guidelines and restrictions:

- 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.
- Tunnel ports are not trunks. Any commands to configure trunking are inactive while the port is configured as a tunnel port.
- Tunnel ports learn customer MAC addresses.
- 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.
- By default, the native VLAN traffic of a dot1q trunk is sent untagged, which cannot be double-tagged in the service provider network. Because of this situation, the native VLAN traffic might not be tunneled correctly. Be sure that the native VLAN traffic is always sent tagged in an asymmetrical link. To tag the native VLAN egress traffic and drop all untagged ingress traffic, enter the global **vlan dot1q tag native** command.
- Configure jumbo frame support on tunnel ports:
 - See the “[Configuring Jumbo Frame Support](#)” section on page 9-10.
 - Take note of the modules listed in the “Configuring Jumbo Frame Support” section that do not support jumbo frames.
- 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.
- 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.
- 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.
- The 802.1Q tunneling feature cannot be configured on ports configured to support private VLANs.
- 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)

- Spanning-tree BPDU filtering is enabled automatically on tunnel ports.
- CDP is automatically disabled on tunnel ports.
- 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 [Chapter 22, “Configuring Layer 2 Protocol Tunneling,”](#) for configuration details.

- 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.

The following configuration guidelines are *required* for your Layer 2 protocol tunneling configuration:

- 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 Spanning-tree BPDU filtering is enabled automatically on tunnel ports.

- 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.
- 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
```

- 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.

The following configuration guidelines are *optional* for your Layer 2 protocol tunneling configuration:

- 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:

- [Configuring 802.1Q Tunnel Ports, page 21-6](#)
- [Configuring the Switch to Tag Native VLAN Traffic, page 21-7](#)



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.

Configuring 802.1Q Tunnel Ports

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

	Command	Purpose
Step 1	Router(config)# interface <i>type</i> ¹ <i>slot/port</i>	Selects the LAN port to configure.
Step 2	Router(config-if)# switchport	Configures the LAN port for Layer 2 switching. <ul style="list-style-type: none"> • You must enter the switchport command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional switchport commands with keywords. • Required only if you have not entered the switchport command already for the interface.
Step 3	Router(config-if)# switchport mode dot1q-tunnel	Configures the Layer 2 port as a tunnel port.
Step 4	Router(config-if)# end	Exits configuration mode.
Step 5	Router# show dot1q-tunnel [{ interface <i>type</i> ¹ <i>interface-number</i> }]	Verifies the configuration.

1. *type* = **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 dot1q-tunnel
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.

On ports where you enter the `no switchport trunk native vlan tag` interface command, the function of the `vlan dot1q tag native` global command is disabled.

These sections describe how to configure the switch to tag native VLAN traffic:

- [Configuring the Switch to Tag Native VLAN Traffic Globally, page 21-7](#)
- [Configuring Ports Not to Tag Native VLAN Traffic, page 21-7](#)

Configuring the Switch to Tag Native VLAN Traffic Globally

With Release 12.2(33)SXH and later releases, to configure the switch to tag traffic in the native VLAN globally, perform this task:

	Command	Purpose
Step 1	Router(config)# <code>vlan dot1q tag native</code>	Configures the switch to tag native VLAN traffic globally.
Step 2	Router(config)# <code>end</code>	Exits configuration mode.
Step 3	Router# <code>show vlan dot1q tag native include globally</code>	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 | include globally
dot1q native vlan tagging is enabled globally
Router(config)#
```

Configuring Ports Not to Tag Native VLAN Traffic

When the switch is configured to tag native VLAN traffic globally, you can disable native VLAN tagging on a per-port basis.

To configure a port not to tag traffic in the native VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# <code>interface type¹ slot/port</code>	Selects the LAN port to configure.
Step 2	Router(config-if)# <code>switchport</code>	Configures the LAN port for Layer 2 switching. <ul style="list-style-type: none"> • You must enter the <code>switchport</code> command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional <code>switchport</code> commands with keywords. • Required only if you have not entered the <code>switchport</code> command already for the port.

	Command	Purpose
Step 3	Router(config-if)# no switchport trunk native vlan tag	Configures the Layer 2 port not to tag native VLAN traffic.
Step 4	Router(config-if)# end	Exits configuration mode.
Step 5	Router# show interface type¹ interface-number include tagging	Verifies the configuration.

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

**Note**

The **switchport trunk native vlan tag** interface command does not enable native VLAN tagging unless the switch is configured to tag native VLAN traffic globally.

This example shows how to configure Gigabit Ethernet port 1/4 to tag traffic in the native VLAN and verify the configuration:

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/4
Router(config-if)# switchport trunk native vlan tag
Router(config-if)# end
Router# show interface gigabitethernet 1/4 switchport | include tagging
Administrative Native VLAN tagging: enabled
Operational Native VLAN tagging: disabled
Router#
```

**Tip**

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html