



IEEE 802.1Q Tunneling

Last Updated: January 29, 2013

The IEEE 802.1Q Tunneling feature provides a single VLAN to support multiple customer VLANs, while preserving customer VLAN IDs and segregating traffic in different customer VLANs.

This module describes the IEEE 802.1Q Tunneling feature and explains how to configure IEEE 802.1Q tunneling in Cisco software.

- [Finding Feature Information, page 1](#)
- [Restrictions for IEEE 802.1Q Tunneling, page 1](#)
- [Information About IEEE 802.1Q Tunneling, page 2](#)
- [How to Configure IEEE 802.1Q Tunneling, page 4](#)
- [Configuration Examples for IEEE 802.1Q Tunneling, page 5](#)
- [Additional References for IEEE 802.1Q Tunneling, page 5](#)
- [Feature Information for IEEE 802.1Q Tunneling, page 6](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IEEE 802.1Q Tunneling

- Only asymmetrical links can be used to direct traffic into a tunnel or to remove traffic from a tunnel.
- The native VLAN traffic should always be sent untagged in an asymmetrical link, for IEEE 802.1Q tunneling to be configured.
- Asymmetrical links do not support the Dynamic Trunking Protocol (DTP) because only one port on the link is a trunk.



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

- The IEEE 802.1Q Tunneling feature cannot be configured on ports that are configured to support private VLANs.

Information About IEEE 802.1Q Tunneling

- [Overview of IEEE 802.1Q Tunneling, page 2](#)
- [IEEE 802.1Q Tunnel Ports, page 2](#)

Overview of IEEE 802.1Q Tunneling

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 (class of service) and the VLAN. The received customer traffic is added to 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 that carries tunnel traffic is an 802.1Q tunnel. The tunnel ports in the VLAN are the tunnel's ingress and egress points.

**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.

A port configured to support an 802.1Q tunnel is called a tunnel port. When you configure a tunnel, 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 that supports all the VLANs that the customer uses. 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.

IEEE 802.1Q tunneling enables the use of a single VLAN to support multiple customer VLANs. The customer switches are trunk connected, but with IEEE 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. The IEEE 802.1Q Tunneling feature 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.

IEEE 802.1Q Tunnel Ports

In the IEEE 802.1Q Tunneling feature, tagged customer traffic comes from an 802.1Q trunk port on a customer device and enters the service-provider edge device 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 the two figures below to understand more about IEEE 802.1 tunnel port connections.

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

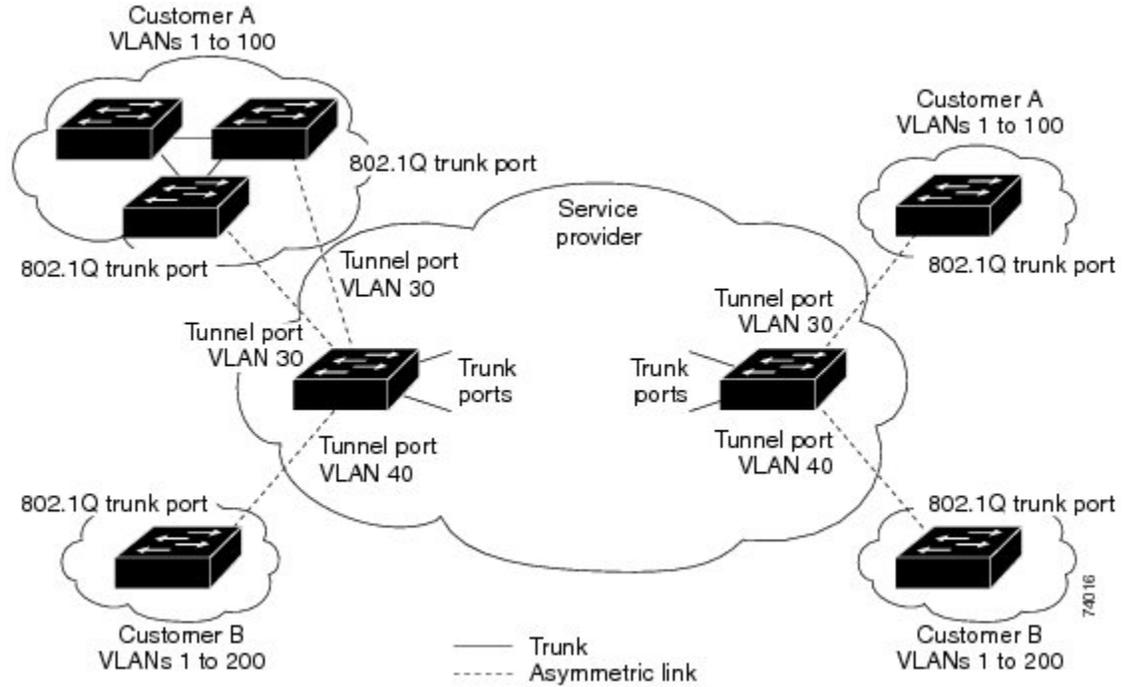
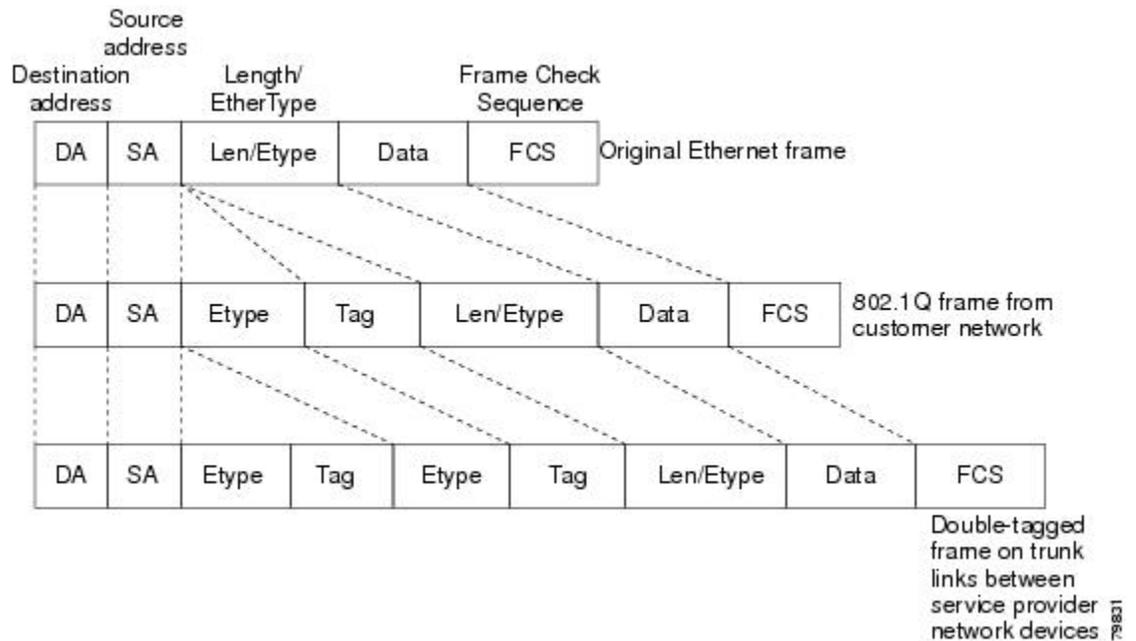


Figure 2 Untagged, 802.1Q-Tagged, and Double-Tagged Ethernet Frames



How to Configure IEEE 802.1Q Tunneling

- [Configuring IEEE 802.1Q Tunnel Ports, page 4](#)

Configuring IEEE 802.1Q Tunnel Ports

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **switchport**
5. **mode dot1q-tunnel**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface gigabitethernet 1/0/0	Enters interface configuration mode.
Step 4	switchport Example: Device(config-if)# switchport	Configures the LAN port for Layer 2 switching.

Command or Action	Purpose
Step 5 <code>mode dot1q-tunnel</code> Example: Device(config-if)# mode dot1q-tunnel	Configures the Layer 2 port as a tunnel port.
Step 6 <code>end</code> Example: Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for IEEE 802.1Q Tunneling

- [Example: Configuring IEEE 802.1Q Tunnel Ports, page 5](#)

Example: Configuring IEEE 802.1Q Tunnel Ports

This example shows how to configure IEEE 802.1Q Tunneling on the Fast Ethernet interface 4/1:

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

Additional References for IEEE 802.1Q Tunneling

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Command List, All Releases
IP LAN switching commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS LAN Switching Services Command Reference

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for IEEE 802.1Q Tunneling

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 *Feature Information for IEEE 802.1Q Tunneling*

Feature Name	Releases	Feature Information
IEEE 802.1Q Tunneling	Cisco IOS XE Release 2.1	<p>The IEEE 802.1Q Tunneling feature lets you use a single VLAN to support multiple customer VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated.</p> <p>The following command was introduced: mode dot1q-tunnel</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.