



Configuring IEEE 802.1Q Tunneling

This chapter describes how to configure IEEE 802.1Q tunneling on the Catalyst 6000 family switches.

This chapter consists of these sections:

- [Understanding How 802.1Q Tunneling Works, page 7-1](#)
- [802.1Q Tunneling Configuration Guidelines, page 7-2](#)
- [Configuring Support for 802.1Q Tunneling, page 7-3](#)

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. To keep customer traffic segregated, each customer requires a separate VLAN, but that one VLAN supports all of the customer's VLANs.

With 802.1Q tunneling, tagged traffic comes from an 802.1Q trunk port on a customer device and enters the 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.

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 1-byte Ethertype field (0x8100) and a 1-byte length field and puts the received customer traffic 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 1-byte Ethertype field (0x8100) and the 1-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.

802.1Q Tunneling Configuration Guidelines

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

- 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. You must enter the global **set dot1q-all-tagged enable** command to ensure that egress traffic in the native VLAN is tagged with 802.1Q tags.
- Because tunnel traffic retains the 802.1Q tag within the switch, the Layer 2 frame header length imposes the following restrictions:
 - The Layer 3 packet within the Layer 2 frame cannot be identified.
 - Layer 3 and higher parameters are not identifiable in tunnel traffic (for example, Layer 3 destination and source addresses).
 - Tunnel traffic cannot be routed.
 - The switch can filter tunnel traffic using only Layer 2 parameters (VLANs and source and destination MAC addresses).
 - The switch can provide only MAC-layer QoS for tunnel traffic.
 - QoS cannot detect the received CoS value in the 802.1Q 2-byte Tag Control Information field.
- 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 with the **nonegotiate dot1q** trunking keywords.
- 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.
- 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
 - Voice over IP (Cisco IP Phone 7960)
- The following Layer 2 protocols work between devices connected by an asymmetrical link:
 - CDP
 - UniDirectional Link Detection (UDLD)
 - Port Aggregation Protocol (PAgP)

- VLAN Trunk Protocol (VTP) does not work between the following devices:
 - Devices connected by an asymmetrical link
 - Devices communicating through a tunnel

**Note**

To configure an EtherChannel as an asymmetrical link, all ports in the EtherChannel must have the same tunneling configuration. Since the Layer 3 packet within the Layer 2 frame cannot be identified, configure the EtherChannel to use MAC-address-based frame distribution.

- Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) works between devices communicating through a tunnel, but does not work between devices connected by an asymmetrical link.
- An interconnected network cannot have redundant paths to two different edge switches in an ISP. An interconnected network may have redundant paths to the same edge switch in an ISP, but the customer network must use Per VLAN Spanning Tree + (PVST+) and cannot be configured for Multi-Instance Spanning Tree Protocol (MISTP). The ISP infrastructure must use either PVST+ or MISTP-PVST+.

Configuring Support for 802.1Q Tunneling

These sections describe 802.1Q tunneling configuration:

- [Configuring the Switch to Support 802.1Q Tunneling, page 7-3](#)
- [Configuring 802.1Q Tunnel Ports, page 7-4](#)
- [Clearing 802.1Q Tunnel Ports, page 7-4](#)
- [Removing Global Support for 802.1Q Tunneling, page 7-4](#)

**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 the Switch to Support 802.1Q Tunneling

The **set dot1q-all-tagged enable** command is a global command that configures a switch to forward all frames from 802.1Q trunks with 802.1Q tagging, including traffic in the native VLAN, and admit only 802.1Q tagged frames on 802.1Q trunks, dropping any untagged traffic, including untagged traffic in the native VLAN. You can enter this command on any switch that needs to support 802.1Q tunneling with 802.1Q trunks.

To configure the switch to support 802.1Q tunneling, perform this task in privileged mode:

	Task	Command
Step 1	Configure tunneling support on the switch.	set dot1q-all-tagged enable [all]
Step 2	Verify the configuration.	show dot1q-all-tagged

This example shows how to configure tunneling on the switch and verify the configuration:

```
Console> (enable) set dot1q-all-tagged enable
Dot1q tagging is enabled
Console> (enable) show dot1q-all-tagged
Dot1q all tagged mode enabled
Console> (enable)
```

Configuring 802.1Q Tunnel Ports

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

	Task	Command
Step 1	Configure tunneling on a port.	set port dot1qtunnel {mod/port} access
Step 2	Verify the configuration.	show port dot1qtunnel [mod[/port]]

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

```
Console> (enable) set port dot1qtunnel 4/1 access
Dot1q tunnel feature set to access mode on port 4/1.
Port 4/1 trunk mode set to off.
Console> (enable) show port dot1qtunnel 4/1
Port   Dot1q tunnel mode
-----
4/1   access
```

Clearing 802.1Q Tunnel Ports

To clear 802.1Q tunneling support from a port, perform this task in privileged mode:

	Task	Command
Step 1	Clear tunneling from a port.	set port dot1qtunnel {mod/port} disable
Step 2	Verify the configuration.	show port dot1qtunnel [mod[/port]]

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

```
Console> (enable) set port dot1qtunnel 4/1 disable
Dot1q tunnel feature disabled on port 4/1.
Console> (enable) show port dot1qtunnel 4/1
Port   Dot1q tunnel mode
-----
4/1   disabled
```

Removing Global Support for 802.1Q Tunneling

You do not need to enter the **set dot1q-all-tagged disable** command to clear 802.1Q tunneling. The **set port dot1qtunnel disable** command is the only command required to clear the feature from the port.

To remove global support for 802.1Q tunneling on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Remove tunneling support on the switch.	set dot1q-all-tagged disable [all]
Step 2	Verify the configuration.	show dot1q-all-tagged

This example shows how to remove tunneling support on the switch and verify the configuration:

```
Console> (enable) set dot1q-all-tagged disable  
Dot1q tagging is disabled  
Console> (enable) show dot1q-all-tagged  
Dot1q all tagged mode disabled  
Console> (enable)
```

