



Configuring 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 Command Reference* publication.

This chapter consists of these sections:

- [Understanding How 802.1Q Tunneling Works, page 7-1](#)
- [802.1Q Tunneling Configuration Guidelines, page 7-2](#)
- [Configuring 802.1Q Tunneling on the Switch, page 7-4](#)
- [Understanding How Layer 2 Protocol Tunneling Works, page 7-6](#)
- [Layer 2 Protocol Tunneling Configuration Guidelines, page 7-7](#)
- [Configuring Support for Layer 2 Protocol Tunneling, page 7-7](#)

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 that is 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 that carries 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.

Not all switches support the standard 1-byte Ethertype field (0x8100). If your switch does not support the 1-byte Ethertype field, you can connect the switch to a Gigabit Interface Converter (GBIC) or 10-Gigabit port and separate untagged IP traffic from the IP management traffic with a specified Ethertype. The untagged IP traffic is automatically assigned to the native VLAN, and the traffic with the specified Ethertype is switched to a specified VLAN.

802.1Q Tunneling Configuration Guidelines

This section provides the guidelines for 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 tunnel ports only to VLANs that are 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 nontunnel port.
- 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 quality of service (QoS) for tunnel traffic.
 - QoS cannot detect the received class of service (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.
- 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 **set dot1q-all-tagged enable** command to ensure that egress traffic in the native VLAN is tagged with 802.1Q tags.



Note See Chapter 5, “Configuring Ethernet VLAN Trunks,” for information on using the global **set dot1q-all-tagged enable** command.

- 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.
- You can tunnel jumbo frames if the jumbo frame length combined with the 802.1Q tag does not exceed the maximum frame size.

**Note**

In order to set the correct maximum transmission unit (MTU) size, you must enable jumbo frames on all ports that carry 802.1 tunnel traffic.

- You cannot configure the 802.1Q tunneling feature on ports that are configured to support the following:
 - Private VLANs
 - Voice over IP (Cisco IP Phone 7960)
- The following Layer 2 protocols work between devices that are connected by an asymmetrical link:
 - CDP
 - UniDirectional Link Detection (UDLD)
 - Port Aggregation Protocol (PAgP)
- VLAN Trunking Protocol (VTP) does not work between the following devices:
 - Devices that are 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. Because 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 that communicate through a tunnel but does not work between devices that are connected by an asymmetrical link.

- An interconnected network cannot have redundant paths to two different edge switches in an ISP. An interconnected network can have redundant paths to the same edge switch in an ISP, but the customer network must use Per VLAN Spanning Tree + (PVST+); it cannot be configured for Multi-Instance Spanning Tree Protocol (MISTP) or Multiple Spanning Tree (MST). The ISP infrastructure must use either PVST+, MISTP-PVST+, or MST-PVST+.

Configuring 802.1Q Tunneling on the Switch

These sections describe how to configure 802.1Q tunneling:

- [Configuring 802.1Q Tunnel Ports, page 7-4](#)
- [Clearing 802.1Q Tunnel Ports, page 7-4](#)
- [Disabling Global Support for 802.1Q Tunneling, page 7-5](#)



Note

See [Chapter 5, “Configuring Ethernet VLAN Trunks,”](#) for information on using the global `set dot1q-all-tagged enable` command.

Configuring 802.1Q Tunnel Ports



Caution

When you are configuring tunneling in any VLAN, make sure that you configure only the appropriate tunnel ports and that you use one VLAN for each tunnel. Incorrect assignment of tunnel ports to VLANs can cause traffic forwarding problems.

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

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

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

```

Disabling Global Support for 802.1Q Tunneling

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

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

	Task	Command
Step 1	Disable global tunneling support on the switch.	set port dot1qtunnel all disable
Step 2	Verify the configuration.	show port dot1qtunnel

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

```

Console> (enable) set port dot1qtunnel all disable
Dot1q tunnel feature disabled on all applicable ports.
Console> (enable) show port dot1qtunnel
Port   Dot1q tunnel mode
-----
2/1    disabled
2/2    disabled
3/1    disabled
3/2    disabled
3/3    disabled
3/4    disabled
3/5    disabled
3/6    disabled
3/7    disabled
3/8    disabled
3/9    disabled
3/10   disabled
3/11   disabled
3/12   disabled
3/13   disabled
3/14   disabled
3/15   disabled
3/16   disabled
<output truncated>

```

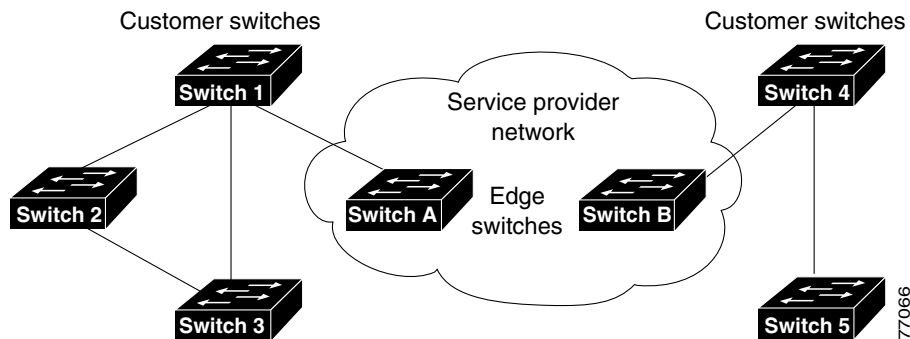
Understanding How Layer 2 Protocol Tunneling Works

Layer 2 protocol tunneling allows the protocol data units (PDUs) (CDP, STP, and VTP) to be tunneled through a network. Some terminology that is used in this section is defined as follows:

- Edge switch—The switch connected to the customer switch and placed on the boundary of the service provider network (see [Figure 7-1](#)).
- Layer 2 protocol tunnel port—A port on the edge switch on which a specific tunneled protocol can be encapsulated or deencapsulated. The tunnel port is configured through CLI commands.
- Tunneled PDU—A CDP, STP, or VTP PDU.

In the current implementation of 802.1Q tunneling, spanning tree BPDUs are flooded only on the special 802.1Q tunnel ports that belong to the same edge switch. This implementation prevents loops between the edge switch and the customer switch at each site. The BPDUs are not flooded on the ports that are connected to other service provider switches inside the service provider network. This handling of the BPDUs creates different spanning tree domains (different spanning tree roots) for the customer network. For example, STP for a VLAN on switch 1 (see [Figure 7-1](#)) builds a spanning tree topology on Switches 1, 2, and 3 without considering the convergence parameters that are 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 Layer 2 protocol tunneling.

Figure 7-1 Layer 2 Protocol Tunneling Network Configuration



Layer 2 protocol tunneling 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 that are received on a tunneled port with the Cisco proprietary multicast address (01-00-0c-cd-cd-d0). The PDU is then flooded to the native VLAN of the tunneled port. If you enable Layer 2 protocol tunneling on a port, the 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.

Layer 2 Protocol Tunneling Configuration Guidelines

This section provides the guidelines for configuring protocol tunneling in your network:

- Protocol tunneling functions independently from the 802.1Q tunneling feature that was described in the previous sections.
- For performance reasons, we do not recommend that you configure Layer 2 protocol tunneling in systems with a Supervisor Engine 1.
- You can enable Layer 2 protocol tunneling on access ports, trunk ports, or 802.1Q tunneling ports only.
- Layer 2 protocol tunneling is not supported with private VLANs.
- Layer 2 protocol tunneling is not supported with dynamic VLANs.
- If you are running MST and connecting to an ISP network using EtherChannels, you must set the link type to **shared** on all the channeling ports by using the **set spantree mst link-type mod/port shared** command. This prevents the EtherChannels from going into the errdisable state because of channel misconfiguration.

Configuring Support for Layer 2 Protocol Tunneling

These sections describe protocol tunneling configuration:

- [Specifying a Layer 2 Protocol, page 7-7](#)
- [Specifying Drop and Shutdown Thresholds on Layer 2 Protocol Tunneling Ports, page 7-9](#)
- [Specifying CoS on Layer 2 Protocol Tunneling Ports, page 7-10](#)
- [Clearing Layer 2 Protocol Tunneling Statistics, page 7-10](#)

Specifying a Layer 2 Protocol

To specify a Layer 2 protocol on a port or range of ports, perform this task in privileged mode:

	Task	Command
Step 1	Specify a Layer 2 protocol on a port.	set port l2protocol-tunnel <i>mod/port</i> { cdp stp vtp } { enable disable }
Step 2	Verify the configuration.	show l2protocol-tunnel statistics [<i>mod[/port]</i>]

This example shows how to specify a Layer 2 protocol on a port and verify the configuration:



Note

You can specify more than one protocol type at a time. In the CLI, separate protocol types with a space.

```
Console> (enable) set port l2protocol-tunnel 3/15 cdp enable
Layer 2 protocol tunneling enabled for CDP on port 3/15.
Port 3/15 trunk mode set to off.
```

```
Console> (enable) set port l2protocol-tunnel 3/15 cdp disable
Layer 2 protocol tunneling disabled for CDP on port 3/15.
```

```
Console> (enable) set port l2protocol-tunnel 3/15 cdp stp vtp enable
Layer 2 protocol tunneling enabled for CDP STP VTP on port 3/15.
Port 3/15 trunk mode set to off.
```

```
Console> (enable) show l2protocol-tunnel statistics 3/15
Tunneling CoS is set to 5.
```

Port	CDP Frames Encap	CDP Frames De-encap
3/15	97465	94434

Port	STP Frames Encap	STP Frames De-encap
3/15	67465	34434

Port	VTP Frames Encap	VTP Frames De-encap
3/15	1212	1213

```
Console> (enable)
```

Configuring Layer 2 Protocol Tunneling on Trunks

Layer 2 protocol tunneling on trunks allows third-party vendors' equipment to interoperate with the Catalyst 6500 series switch in service-provider networks. Layer 2 protocol tunneling makes control protocol PDUs such as STP, CDP, and VTP, transparent to the service provider cloud when passing traffic through trunk ports. In earlier releases, Layer 2 protocol tunneling was available on access ports only.

Follow the guidelines that are described in the [“Layer 2 Protocol Tunneling Configuration Guidelines” section on page 7-7](#). Additionally, you cannot configure 802.1Q tunneling on trunk ports; however, 802.1Q tunneling can be tunneled through trunk ports.



Note

If you have a mixed network environment that is using both 802.1Q tunneling and Layer 2 protocol tunneling, you must double tag packets in order to interoperate with third-party equipment.

To enable or disable Layer 2 protocol tunneling on a port or range of ports, perform this task in privileged mode:

Task	Command
Enable or disable Layer 2 protocol tunneling on a trunk.	set l2protocol-tunnel trunk {enable disable}



Note

Do not configure (enable or disable) Layer 2 protocol tunneling on trunks when active layer 2 protocol tunnels are already configured. If you plan to configure Layer 2 protocol tunneling on trunks, do so before performing any other Layer 2 protocol tunneling tasks.

This example shows how to enable Layer 2 protocol tunneling on a trunk:

```
Console> (enable) set l2protocol-tunnel trunk enable
Layer 2 Protocol Tunnel on trunks is allowed.
```

This example shows how to enable Layer 2 protocol tunneling on a trunk:

```
Console> (enable) set l2protocol-tunnel trunk disable
Warning!! Clear any layer 2 protocol tunnel configuration on trunks
before using this command.
Layer 2 Protocol Tunnel on trunks is not allowed.
```

Specifying Drop and Shutdown Thresholds on Layer 2 Protocol Tunneling Ports

The shutdown threshold provides a type of rate limiting that prevents the edge switch from being overwhelmed by attached customer switches. We recommend that you configure a shutdown threshold value whenever you use Layer 2 protocol tunneling ports with 802.1Q tunneling.

We recommend 1000 as a maximum value for the shutdown threshold. This value reflects the number of PDUs that an edge switch can handle per second (without dropping any) while performing egress and ingress tunneling. For an edge switch, the shutdown threshold value also determines the number of Layer 2 protocol tunneling ports that can be connected to customer switches and the number of customer VLANs per Layer 2 protocol tunneling port. In determining the recommended maximum value of 1000, egress tunneling from the service provider network was also taken into consideration.

To determine the number of Layer 2 protocol tunneling ports (links) and the number of customer VLANs per Layer 2 protocol tunneling port (VLANs per link) that an edge switch can handle, multiply the number of Layer 2 protocol tunneling ports by the number of VLANs and the result should be less than or equal to 1000. Some examples of acceptable configurations are as follows:

- 1 Layer 2 protocol tunneling port x 1000 VLANs
- 2 Layer 2 protocol tunneling port x 500 VLANs
- 5 Layer 2 protocol tunneling port x 200 VLANs
- 10 Layer 2 protocol tunneling port x 100 VLANs
- 20 Layer 2 protocol tunneling port x 50 VLANs
- 100 Layer 2 protocol tunneling port x 10 VLANs



Note

After reaching the shutdown threshold factor, the port or range of ports goes into the errdisable state and is restored after the errdisable timeout interval. The shutdown threshold factor should exceed the drop threshold factor. After reaching the drop threshold factor, the port or range of ports starts dropping PDUs.

The default for the drop threshold and the shutdown threshold is 0, 0, which indicates that no limit is set.

To specify the drop and shutdown thresholds on a port, perform this task in privileged mode:

	Task	Command
Step 1	Specify the drop and shutdown thresholds on a port.	set port l2protocol-tunnel <i>mod/port</i> { drop-threshold <i>drop-threshold</i> } { shutdown-threshold <i>shutdown-threshold</i> }
Step 2	Verify the configuration.	show port l2protocol-tunnel [<i>mod/port</i>]

This example shows how to specify the drop threshold to 1000 and the shutdown threshold to 1000 on a port:

```

Console> (enable) set port l2protocol-tunnel 3/15 drop-threshold 1000 shutdown-threshold
1000
Drop Threshold=1000, Shutdown Threshold=1000 set on port 3/15.
Console> (enable)

Console> (enable) show port l2protocol-tunnel 3/15
Port Tunnel Protocol(s) Drop Threshold Shutdown Threshold
-----
3/15 CDP, STP, VTP 1000 1000
Console> (enable)

```

Specifying CoS on Layer 2 Protocol Tunneling Ports

You can specify a class of service (CoS) value globally on all ingress Layer 2 protocol tunneling ports. Because the CoS value applies to all ingress tunneling ports, all encapsulated PDUs that are sent out by the switch have the same CoS value. Valid values are 0 to 7 and the default CoS is 5.

To specify a CoS value globally on all ingress Layer 2 protocol tunneling ports, perform this task in privileged mode:

	Task	Command
Step 1	Globally specify a CoS value.	set l2protocol-tunnel cos <i>cos-value</i>
Step 2	Verify the configuration.	show l2protocol-tunnel statistics [<i>mod[/port]</i>]

This example shows how to set the CoS value to 6:

```

Console> (enable) set l2protocol-tunnel cos 6
New CoS value is 6.
Console> (enable)

Console> (enable) show l2protocol-tunnel statistics 4/1
Tunneling CoS is set to 6.
Port CDP Frames Encap CDP Frames De-encap
-----
4/1 97465 94434
.
.
.
console> (enable)

Console> (enable) clear l2protocol-tunnel cos
Default Cos set to 5.
Console> (enable)

```

Clearing Layer 2 Protocol Tunneling Statistics

To clear Layer 2 protocol tunneling statistics on a port or on all tunneling ports, perform this task in privileged mode:

Task	Command
Clear Layer 2 tunnel port statistics.	clear l2protocol-tunnel statistics [<i>mod/port</i>]

This example shows how to clear Layer 2 tunnel port statistics on port 7/1:

```
Console> (enable) clear l2protocol-tunnel statistics 7/1  
Layer 2 Protocol Tunnel statistics cleared on ports: 7/1.  
Console> (enable)
```

