



# CHAPTER 14

## Configuring IEEE 802.1Q Tunneling, VLAN Mapping, 802.1ad, and Layer 2 Protocol Tunneling

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks. Tunneling is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. The Cisco ME 3400E Ethernet Access switch supports IEEE 802.1Q tunneling and Layer 2 protocol tunneling. It also supports VLAN mapping (or VLAN ID translation) on trunk ports.



### Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

- [Understanding 802.1Q Tunneling, page 14-1](#)
- [Configuring 802.1Q Tunneling, page 14-4](#)
- [Understanding VLAN Mapping, page 14-7](#)
- [Configuring VLAN Mapping, page 14-9](#)
- [Configuring IEEE 802.1ad, page 14-13](#)
- [Understanding Layer 2 Protocol Tunneling, page 14-20](#)
- [Configuring Layer 2 Protocol Tunneling, page 14-22](#)
- [Monitoring and Maintaining Tunneling and Mapping Status, page 14-30](#)

## Understanding 802.1Q Tunneling

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the 802.1Q specification.

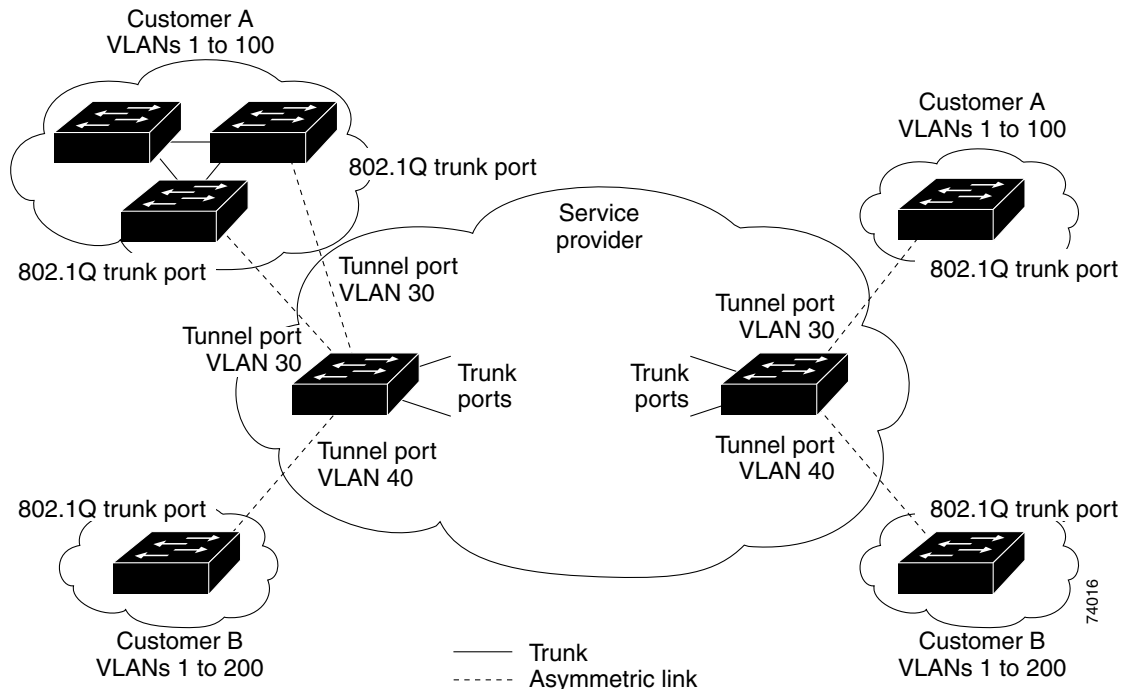
Using the 802.1Q tunneling (QinQ) feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs (C-VLANs) are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using 802.1Q tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. 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 ID that is dedicated to tunneling. Each customer requires a separate service-provider VLAN ID (S-VLAN), but that VLAN ID supports all of the customer's VLANs. Configuring 802.1Q tunneling on a tunnel port is referred to as *traditional QinQ*.

Customer traffic tagged in the normal way with appropriate VLAN IDs comes from an 802.1Q trunk port on the customer device and into a tunnel port on the service-provider edge switch. The link between the customer device and the edge switch is asymmetric 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 interface to an access VLAN ID that is unique to each customer. See Figure 14-1.

**Note**

By default, VLANs configured on the switch are user network interface-enhanced network interface (UNI-ENI) isolated VLANs. In a UNI-ENI isolated VLAN, 802.1Q tunneled access ports on the switch are isolated from each other. If you use the **uni-vlan community** VLAN configuration command to change a VLAN to a UNI-ENI community VLAN, local switching occurs between these ports. For more information about UNI-ENI VLANs, see Chapter 12, “Configuring VLANs.”

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



Packets coming from the customer trunk port into the tunnel port on the service-provider edge switch are normally 802.1Q-tagged with the appropriate VLAN ID. The the tagged packets remain intact inside the switch and when they exit the trunk port into the service-provider network, they are encapsulated with another layer of an 802.1Q tag (called the *metro tag*) that contains the VLAN ID that is unique to

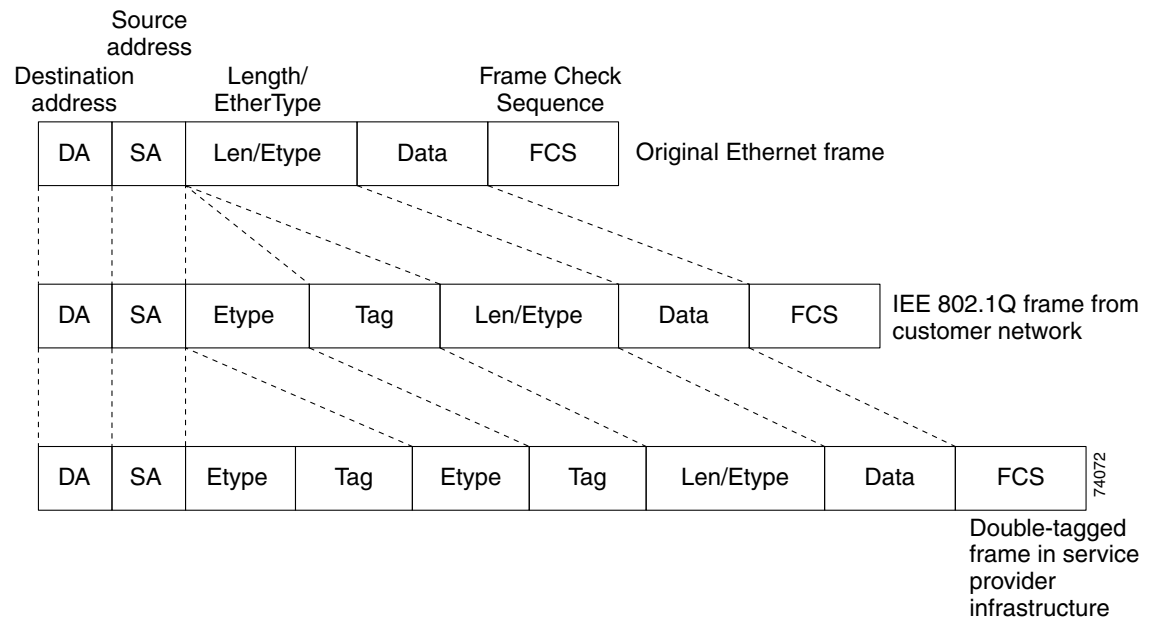
the customer. The original customer 802.1Q tag is preserved in the encapsulated packet. Therefore, packets entering the service-provider network are double-tagged, with the outer (metro) tag containing the customer's access VLAN ID, and the inner VLAN ID being that of the incoming traffic.

When the double-tagged packet enters another trunk port in a service-provider core switch, the outer tag is stripped as the switch processes the packet. When the packet exits another trunk port on the same core switch, the same metro tag is again added to the packet. [Figure 14-2](#) shows the tag structures of the double-tagged packets.

**Note**

Remove the Layer 2 protocol configuration from a trunk port because incoming encapsulated packets change that trunk port to error disabled. The outgoing encapsulated VTP (CDP and STP) packets are dropped on that trunk.

**Figure 14-2 Original (Normal), 802.1Q, and Double-Tagged Ethernet Packet Formats**



When the packet enters the trunk port of the service-provider egress switch, the outer tag is again stripped as the switch internally processes the packet. However, the metro tag is not added when the packet is sent out the tunnel port on the edge switch into the customer network. The packet is sent as a normal 802.1Q-tagged frame to preserve the original VLAN numbers in the customer network.

In [Figure 14-1](#), Customer A was assigned VLAN 30, and Customer B was assigned VLAN 40. Packets entering the edge switch tunnel ports with 802.1Q tags are double-tagged when they enter the service-provider network, with the outer tag containing VLAN ID 30 or 40, appropriately, and the inner tag containing the original VLAN number, for example, VLAN 100. Even if both Customers A and B have VLAN 100 in their networks, the traffic remains segregated within the service-provider network because the outer tag is different. Each customer controls its own VLAN numbering space, which is independent of the VLAN numbering space used by other customers and the VLAN numbering space used by the service-provider network.

At the outbound tunnel port, the original VLAN numbers on the customer's network are recovered. It is possible to have multiple levels of tunneling and tagging, but the switch supports only one level in this release.

If traffic coming from a customer network is not tagged (native VLAN frames), these packets are bridged or routed as normal packets. All packets entering the service-provider network through a tunnel port on an edge switch are treated as untagged packets, whether they are untagged or already tagged with 802.1Q headers. The packets are encapsulated with the metro tag VLAN ID (set to the access VLAN of the tunnel port) when they are sent through the service-provider network on an 802.1Q trunk port. The priority field on the metro tag is set to the interface class of service (CoS) priority configured on the tunnel port. (The default is zero if none is configured.)

## Configuring 802.1Q Tunneling

- [Default 802.1Q Tunneling Configuration, page 14-4](#)
- [802.1Q Tunneling Configuration Guidelines, page 14-4](#)
- [802.1Q Tunneling and Other Features, page 14-6](#)
- [Configuring an 802.1Q Tunneling Port, page 14-6](#)

### Default 802.1Q Tunneling Configuration

By default, 802.1Q tunneling is disabled because the default switchport mode is access. Tagging of 802.1Q native VLAN packets on all 802.1Q trunk ports is also disabled. By default, VLANs on the switch are UNI-ENI isolated VLANs.

### 802.1Q Tunneling Configuration Guidelines

When you configure 802.1Q tunneling, you should always use an asymmetrical link between the customer device and the edge switch, with the customer device port configured as an 802.1Q trunk port and the edge switch port configured as a tunnel port.

Assign tunnel ports only to VLANs that are used for tunneling.

Configuration requirements for native VLANs and for and maximum transmission units (MTUs) are explained in these next sections.

#### Native VLANs

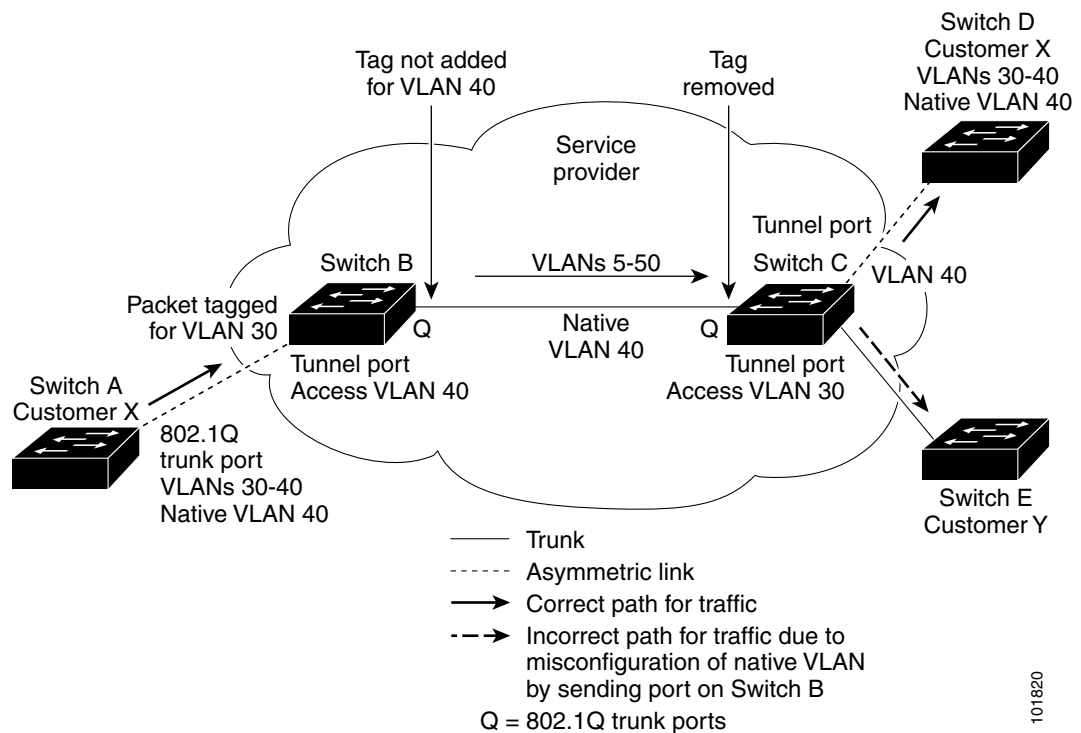
When configuring 802.1Q tunneling on an edge switch, you must use 802.1Q trunk ports for sending packets into the service-provider network. However, packets going through the core of the service-provider network can be carried through 802.1Q trunks, ISL trunks, or nontrunking links. When 802.1Q trunks are used in these core switches, the native VLANs of the 802.1Q trunks must not match any native VLAN of the nontrunking (tunneling) port on the same switch because traffic on the native VLAN would not be tagged on the 802.1Q sending trunk port.

See [Figure 14-3](#). VLAN 40 is configured as the native VLAN for the 802.1Q trunk port from Customer X at the ingress edge switch in the service-provider network (Switch B). Switch A of Customer X sends a tagged packet on VLAN 30 to the ingress tunnel port of Switch B in the service-provider network, which belongs to access VLAN 40. Because the access VLAN of the tunnel port (VLAN 40) is the same as the native VLAN of the edge-switch trunk port (VLAN 40), the metro tag is not added to tagged packets received from the tunnel port. The packet carries only the VLAN 30 tag through the service-provider network to the trunk port of the egress-edge switch (Switch C) and is misdirected through the egress switch tunnel port to Customer Y.

These are some ways to solve this problem:

- Use ISL trunks between core switches in the service-provider network. Although customer interfaces connected to edge switches must be 802.1Q trunks, we recommend using ISL trunks for connecting switches in the core layer. The Cisco ME switch does not support ISL trunks.
- Use the **vlan dot1q tag native** global configuration command to configure the edge switch so that all packets going out an 802.1Q trunk, including the native VLAN, are tagged. If the switch is configured to tag native VLAN packets on all 802.1Q trunks, the switch accepts untagged packets, but sends only tagged packets.
- Ensure that the native VLAN ID on the edge-switch trunk port is not within the customer VLAN range. For example, if the trunk port carries traffic of VLANs 100 to 200, assign the native VLAN a number outside that range.

**Figure 14-3** Potential Problem with 802.1Q Tunneling and Native VLANs



101820

## System MTU

The default system MTU for traffic on the switch is 1500 bytes. You can configure Fast Ethernet ports to support frames larger than 1500 bytes by using the **system mtu** global configuration command. You can configure Gigabit Ethernet ports to support frames larger than 1500 bytes by using the **system mtu jumbo** global configuration command. Because the 802.1Q tunneling feature increases the frame size by 4 bytes when the metro tag is added, you must configure all switches in the service-provider network to be able to process maximum frames by increasing the switch system MTU size to at least 1504 bytes. The maximum allowable system MTU for Gigabit Ethernet interfaces is 9000 bytes; the maximum system MTU for Fast Ethernet interfaces is 1998 bytes.

## 802.1Q Tunneling and Other Features

Although 802.1Q tunneling works well for Layer 2 packet switching, there are incompatibilities between some Layer 2 features and Layer 3 switching.


**Note**

Layer 3 switching is supported only when the metro IP access image is running on the switch.

- A tunnel port cannot be a routed port.
- IP routing is not supported on a VLAN that includes 802.1Q tunnel ports. Packets received from a tunnel port are forwarded based only on Layer 2 information. If routing is enabled on a switch virtual interface (SVI) that includes tunnel ports, untagged IP packets received from the tunnel port are recognized and routed by the switch. Customers can access the internet through its native VLAN. If this access is not needed, you should not configure SVIs on VLANs that include tunnel ports.
- Tunnel ports do not support IP access control lists (ACLs).
- Layer 3 quality of service (QoS) ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports. MAC-based QoS is supported on tunnel ports.
- EtherChannel port groups are compatible with tunnel ports as long as the 802.1Q configuration is consistent within an EtherChannel port group.
- UniDirectional Link Detection (UDLD) is supported on 802.1Q tunnel ports.
- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) are supported only on 802.1Q tunnel ports that are network node interfaces (NNIs) or enhanced network interfaces (ENIs). UNIs do not support PAgP and LACP.
- Loopback detection is supported on 802.1Q tunnel ports.
- When an NNI or ENI port is configured as an 802.1Q tunnel port, spanning-tree bridge protocol data unit (BPDU) filtering is automatically enabled on the interface, and the Cisco Discovery Protocol (CDP) and the Layer Link Discovery Protocol (LLDP) are automatically disabled on the interface. UNIs do not support BPDU filtering, CDP, or LLDP.
- In a UNI-ENI isolated VLAN, 802.1Q tunneled access ports are isolated from each other, but in a UNI-ENI community VLAN, local switching occurs between these ports. For more information about UNI-ENI VLANs, see [Chapter 12, “Configuring VLANs.”](#)

## Configuring an 802.1Q Tunneling Port

Beginning in privileged EXEC mode, follow these steps to configure a port as an 802.1Q tunnel port:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode for the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch. Valid interfaces include physical interfaces and port-channel logical interfaces (port channels 1 to 48).
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.

	Command	Purpose
Step 4	<code>switchport access vlan <i>vlan-id</i></code>	Specify the default VLAN, which is used if the interface stops trunking. This VLAN ID is specific to the particular customer.  <b>Note</b> If the VLAN is a UNI-ENI isolated VLAN, local switching does not occur between UNIs and ENIs on the switch. If the VLAN is a UNI-ENI community VLAN, local switching is allowed.
Step 5	<code>switchport mode dot1q-tunnel</code>	Set the interface as an 802.1Q tunnel port.
Step 6	<code>exit</code>	Return to global configuration mode.
Step 7	<code>vlan dot1q tag native</code>	(Optional) Set the switch to enable tagging of native VLAN packets on all 802.1Q trunk ports. When not set, and a customer VLAN ID is the same as the native VLAN, the trunk port does not apply a metro tag, and packets could be sent to the wrong destination.
Step 8	<code>end</code>	Return to privileged EXEC mode.
Step 9	<code>show running-config</code> <code>show dot1q-tunnel</code>	Display the ports configured for 802.1Q tunneling. Display the ports that are in tunnel mode.
Step 10	<code>show vlan dot1q tag native</code>	Display 802.1Q native VLAN tagging status.
Step 11	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Use the **no switchport mode dot1q-tunnel** interface configuration command to return the port to the default state of access. Use the **no vlan dot1q tag native** global configuration command to disable tagging of native VLAN packets.

This example shows how to configure an interface as a tunnel port, enable tagging of native VLAN packets, and verify the configuration. In this configuration, the VLAN ID for the customer connected to Gigabit Ethernet interface 2 is VLAN 22. This VLAN is by default a UNI-ENI isolated VLAN.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Switch# show dot1q-tunnel interface gigabitethernet0/2
dot1q-tunnel mode LAN Port(s)
-----
Gi0/1

Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

## Understanding VLAN Mapping

Another way to establish S-VLANs is to configure VLAN mapping (or VLAN ID translation) on trunk ports connected to a customer network to map customer VLANs to service-provider VLANs. Packets entering the port are mapped to a service provider VLAN (S-VLAN) based on the port number and the original customer VLAN-ID (C-VLAN) of the packet.

In a typical metro deployment, VLAN mapping takes place on user network interfaces (UNIs) or enhanced network interfaces (ENIs) that face the customer network. However, you are not prevented from configuring VLAN mapping on network node interfaces (NNIs).

Because the VLAN ID is mapped to the S-VLAN on ingress, on the ME-3400E all forwarding operations are performed by using S-VLAN information and not C-VLAN information.

**Note**

When you configure features on a port that has VLAN mapping configured, you always use the S-VLAN (translated VLAN) ID, not the customer VLAN-ID (C-VLAN).

On an interface configured for VLAN mapping, the specified C-VLAN packets are mapped to the specified S-VLAN when they enter the port. Symmetrical mapping back to the customer C-VLAN occurs when packets exit the port.

The switch supports these types of VLAN mapping on UNI trunk ports:

- One-to-one VLAN mapping occurs at the ingress and egress of the port and maps the customer C-VLAN ID in the 802.1Q tag to the service-provider S-VLAN ID. You can also specify that packets with all other VLAN IDs are dropped.
- Selective QinQ maps the specified customer VLANs entering the UNI to the specified S-VLAN ID. The S-VLAN is added to the incoming unmodified C-VLAN. You can also specify that traffic carrying all other customer VLAN IDs is dropped.
- Traditional 802.1Q tunneling (QinQ) performs all-to-one bundling of C-VLAN IDs to a single S-VLAN ID for the port. The S-VLAN is added to the incoming unmodified C-VLAN. You can configure the UNI as an 802.1Q tunnel port for traditional QinQ, or you can configure selective QinQ on trunk ports for a more flexible implementation. Mapping takes place at ingress and egress of the port. All packets on the port are bundled into the specified S-VLAN.

**Note**

Untagged packets enter the switch on the trunk native VLAN and are not mapped.

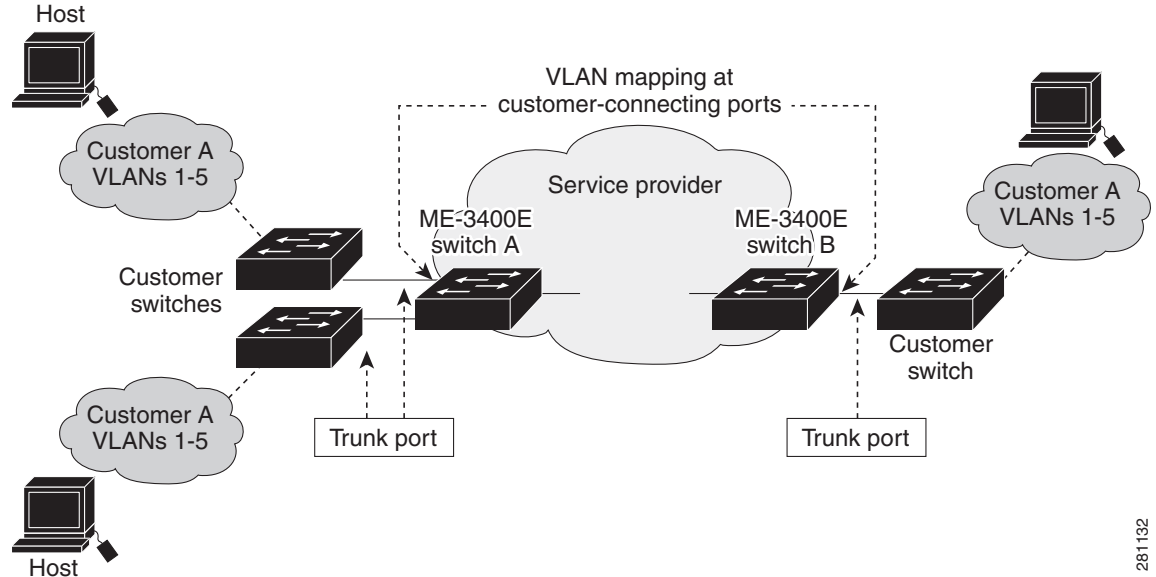
For quality of service (QoS), the switch has flexible mapping between C-CoS or C-DSCP and S-CoS and maps the inner CoS to the outer CoS for traffic with traditional QinQ or selective QinQ VLAN mapping. For more information, see the [“Classification Comparisons” section on page 35-10](#).

## Mapping Customer VLANs to Service-Provider VLANs

[Figure 14-4](#) shows a topology where a customer uses the same VLANs in multiple sites on different sides of a service-provider network. You map the customer VLAN IDs to service-provider VLAN IDs for packet travel across the service-provider backbone. The customer VLAN IDs are retrieved at the other side of the service-provider backbone for use in the other customer site. Configure the same set of VLAN mappings at a customer-connected port on each side of the service-provider network.

See the examples following the configuration steps for using one-to-one mapping, traditional QinQ, or selective QinQ to map customer VLANs 1 to 5 to service-provider VLANs.



**Figure 14-4 Mapping Customer VLANs**

281132

## Configuring VLAN Mapping

- [Default VLAN Mapping Configuration, page 14-9](#)
- [VLAN Mapping Configuration Guidelines, page 14-9](#)
- [Configuring VLAN Mapping, page 14-10](#)

### Default VLAN Mapping Configuration

By default, no VLAN mapping is configured.

### VLAN Mapping Configuration Guidelines

- Traditional QinQ uses 802.1Q tunnel ports; you configure one-to-one VLAN mapping and selective QinQ on 802.1Q trunk ports.
- To avoid mixing customer traffic, when you configure traditional QinQ on a trunk port, you should configure the service provider S-VLAN ID as an allowed VLAN on the trunk port.
- When you configure selective QinQ to tunnel the traffic of two different customers on different S-VLANs, if the native VLAN (VLAN 1) is on one of the selective QinQ interfaces, untagged CDP and STP VLAN 1 packets are leaked to the other customer switches.

The workaround is to use the **switchport trunk native vlan *vlan-id*** interface configuration command to configure the native VLAN ID on an interface tunneling S-VLANs. For example, if you configured QinQ by entering the **switchport vlan mapping 1-100 dot1q-tunnel 500** command, you should also enter the **switchport trunk native vlan 500** command.

- On an ME-3400E interface configured for VLAN mapping, mapping to the S-VLAN occurs on traffic entering the switch. Therefore, when you configure other features on an interface configured for VLAN mapping, you should use the S-VLAN ID, except when configuring VLAN mapping and Ethernet E-LMI. When configuring E-LMI on an interface, use the C-VLAN when entering the **ethernet lmi ce-vlan map** *vlan-id* service instance configuration mode command.
- When you configure VLAN mapping on an EtherChannel, the mapping applies to all ports in the port channel.
- You cannot configure encapsulation replicate on a SPAN destination port if the source port is configured as a tunnel port or has a 1-to-2 mapping configured. Encapsulation replicate is supported with 1-to-1 VLAN mapping.
- To determine switch resources used for VLAN mapping, enter the **show vlan mapping usage** or **show platform vlan mapping** privileged EXEC command.

## Configuring VLAN Mapping

These procedures show how to configure each type of VLAN mapping on trunk ports. To verify your configuration, enter the **show interfaces** *interface-id* **vlan mapping** or **show vlan mapping** privileged EXEC commands. See the “[Monitoring and Maintaining Tunneling and Mapping Status](#)” section on [page 14-30](#) for the syntax of these commands. For more information about all commands in this section, see the command reference for this release.

### Configuring One-to-One Mapping

Beginning in privileged EXEC mode, follow these steps to configure one-to-one VLAN mapping to map a customer VLAN ID to a service-provider VLAN ID. You can use the **default drop** keywords to specify that traffic is dropped unless both the specified C-VLAN ID and S-VLAN ID combination is explicitly mapped.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 3	<b>switchport mode trunk</b>	Configure the interface as a trunk port.
Step 4	<b>switchport vlan mapping</b> <i>vlan-id translated-id</i>	Enter the VLAN IDs to be mapped: <ul style="list-style-type: none"> <li>• <i>vlan-id</i>—the customer VLAN ID (C-VLAN) entering the switch from the customer network. The range is from 1 to 4094.</li> <li>• <i>translated-id</i>—the assigned service-provider VLAN ID (S-VLAN). The range is from 1 to 4094.</li> </ul>
Step 5	<b>switchport vlan mapping default drop</b>	(Optional) Specify that all packets on the port are dropped if they do not match the VLANs specified in Step 4.
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>show vlan mapping</b>	Verify the configuration.
Step 8	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no switchport vlan mapping *vlan-id translated-id*** command to remove the VLAN mapping information. Entering **no switchport vlan mapping all** deletes all mapping configurations.

This example shows how to map VLAN IDs 1 to 5 in the customer network to VLANs 101 to 105 in the service-provider network as shown in Figure 14-4. You configure these same VLAN mapping commands for a port in Switch A and Switch B. The traffic on any other VLAN IDs is dropped.

```
Switch(config)# interface gigabitEthernet0/1
Switch(config-if)# switchport vlan mapping 1 101
Switch(config-if)# switchport vlan mapping 2 102
Switch(config-if)# switchport vlan mapping 3 103
Switch(config-if)# switchport vlan mapping 4 104
Switch(config-if)# switchport vlan mapping 4 105
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

In the previous example, at the ingress of the service-provider network, VLAN IDs 1 to 5 in the customer network are mapped to VLANs 101 to 105, respectively, inside of the service-provider network. At the egress of the service-provider network, VLANs 101 to 105 in the service-provider network are mapped to VLAN IDs 1 to 5, respectively, in the customer network.

## Configuring Traditional QinQ on a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure VLAN mapping for traditional QinQ on a trunk port or tunneling by default. Configuring tunneling by default bundles all packets on the port into the configured S-VLAN.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface-id</i></b>	Enter interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 3	<b>switchport mode trunk</b>	Configure the interface as a trunk port.
Step 4	<b>switchport trunk allowed vlan <i>vlan-id</i></b>	Configure the outer VLAN of the service provider network (S-VLAN) to be allowed on the interface. This should be the same outer VLAN ID entered in the next step.
Step 5	<b>switchport vlan mapping default dot1q-tunnel <i>outer vlan-id</i></b>	Configure VLAN mapping so that all packets entering the port are bundled into the specified S-VLAN:  <i>outer-vlan-id</i> —Enter the outer VLAN ID (S-VLAN) of the service-provider network. The range is from 1 to 4094.
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>show interfaces <i>interface-id</i> vlan mapping</b>	Verify the configuration.
Step 8	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no switchport vlan mapping tunnel default *outer vlan-id*** command to remove the VLAN mapping configuration. Entering **no switchport vlan mapping all** deletes all mapping configurations.

This example shows how to bundle all traffic on the port to leave the switch with the S-VLAN ID of 100.

```
Switch(config)# interface gigabitEthernet0/1
Switch(config-if)# switchport mode trunk
```

```
Switch(config-if)# switchport trunk allowed 100
Switch(config-if)# switchport vlan mapping default dot1q-tunnel 100
Switch(config-if)# exit
```

## Configuring Selective QinQ on a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure VLAN mapping for selective QinQ on a trunk port. Note that you can configure one-to-one mapping and selective QinQ on the same interface, but you cannot use the same C-VLAN IDs in both configurations. You can use the **default drop** keywords to specify that traffic is dropped unless the specified C-VLAN ID and S-VLAN ID combination is explicitly mapped.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 3	<b>switchport mode trunk</b>	Configure the interface as a trunk port.
Step 4	<b>switchport vlan mapping</b> <i>vlan-id</i> <b>dot1q-tunnel</b> <i>outer vlan-id</i>	Enter the VLAN IDs to be mapped: <ul style="list-style-type: none"> <li><i>vlan-id</i>—the customer VLAN ID (C-VLAN) entering the switch from the customer network. The range is from 1 to 4094. You can enter a string of VLAN-IDs.</li> <li><i>outer-vlan-id</i>—Enter the outer VLAN ID (S-VLAN) of the service-provider network. The range is from 1 to 4094.</li> </ul>
Step 5	<b>switchport vlan mapping default drop</b>	(Optional) Specify that all packets on the port are dropped if they do not match the VLANs specified in Step 4.
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>show interfaces</b> <i>interface-id</i> <b>vlan mapping</b>	Verify the configuration.
Step 8	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no switchport vlan mapping *vlan-id* dot1q-tunnel *outer vlan-id*** command to remove the VLAN mapping configuration. Entering **no switchport vlan mapping all** deletes all mapping configurations.

This example shows how to configure selective QinQ mapping on the port so that traffic with a C-VLAN ID of 1 to 5 enters the switch with an S-VLAN ID of 100. The traffic of any other VLAN IDs is dropped.

```
Switch(config)# interface gigabitEthernet0/1
Switch(config-if)# switchport vlan mapping 1-5 dot1q-tunnel 100
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

# Configuring IEEE 802.1ad

While QinQ is a Cisco-proprietary system to enable double-tagging to provide VLAN scalability in the provider network, 802.1ad uses standard protocols for VLAN scalability. As with QinQ, data traffic entering from the customer interface is tagged with a service-provider tag. The customer frame crosses the provider network with two tags: the inner tag is the customer tag (C-tag), and the outer tag is the service-provider tag (S-tag). Control packets appear as data inside the provider network.

See this document for a description of IEEE 802.1ad support on Cisco provider bridges with commands:

[http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce\\_cfm-ieee\\_802\\_1ad.html](http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_802_1ad.html)

The Cisco ME 3400E switch supports these features:

- a switchport-based model
- all-to-one bundling
- service multiplexing (complex UNI)
- split horizon (Cisco IOS Release 12.2(55)SE and later)

In 802.1ad, a switchport is configured as either a customer user-network interface (C-UNI), a service-provider UNI (S-UNI), or a network-to-network interface (NNI). Only Layer 2 interfaces can be 802.1ad ports.

- C-UNI—can be either an access port or an 802.1Q trunk port. The port uses the customer bridge addresses. To configure a C-UNI port, enter the **ethernet dot1ad uni c-port** interface configuration command. New keywords added to the **switchport vlan mapping** interface configuration command allow all-to-one or selective bundling capability for customer VLANs when the interface is configured as an 802.1ad trunk C-UNI port.
- S-UNI—an access port that provides the same service to all customer VLANs entering the interface, marking all C-VLANs entering the port with the same S-VLAN. In this mode, the customer's port is configured as a trunk port, and traffic entering the S-UNI is tagged. On S-UNIs, CDP and LLDP are disabled, and STP BPDU filtering and Port Fast are enabled. You can configure the port as an access port only; trunk configuration is not allowed.
  - CFM C-VLAN configuration is not allowed on an S-UNI.
  - On an ME 3400E switch, you enter the **ethernet dot1ad uni s-port** interface configuration command on an access port with an access VLAN.
- NNI—entering the **ethernet dot1ad nni** interface command on a trunk port creates 802.1ad EtherType (0x88a8) and uses S-bridge addresses for CPU-generated Layer 2 protocol PDUs. Only trunk ports can be NNIs. CFM C-VLAN configuration is not allowed on an NNI.

See the command reference for more information on the commands that support this feature.

For information about 802.1ad QoS, see the “[Configuring 802.1ad QoS](#)” section on page 35-90.

- “[802.1ad and Split-Horizon Configuration Guidelines](#)” section on page 14-14
- “[Configuring 802.1ad EtherChannels](#)” section on page 14-15
- “[Configuring 802.1ad Split Horizon](#)” section on page 14-18

## 802.1ad and Split-Horizon Configuration Guidelines

- An S-UNI (isolated or nonisolated port) must be an access port.
- An NNI must be a trunk port. If you enter the **ethernet dot1ad nni** interface configuration command on a port that is not a trunk port, the switchport mode is automatically changed to trunk.
- A C-UNI (isolated or nonisolated port) can be either an access port or a trunk port.
- On Cisco ME 3400 E switches, 802.1ad is a port-based feature. There is no global command for enabling 802.1ad. By default, without 802.1ad, all switchports are traditional 802.1Q ports.
- When 802.1ad is enabled, the tunneling of customer protocol or control traffic is done in software. If the incoming BPDU rate is high, there could be some impact on CPU utilization.
- The switches do not support 802.1ad on EVCs or 802.1ad Layer 3 termination.
- Releases earlier than Cisco IOS Release 12.2(55)SE do not support split horizon on 802.1ad interfaces. The Catalyst 3750 Metro switch does not support 802.1ad split horizon.
- You cannot enable Layer 2 protocol tunneling on 802.1ad interfaces. The features are mutually exclusive.
- ME 3400E switches support a mixed configuration model for 802.1ad that allows traditional QinQ tunnels and 802.1ad tunnels on a bridge at the same time. When configuring a switch in mixed configuration mode, be sure to separate the broadcast domains for traditional 802.1Q tunneling and 802.1ad tunneling. To ensure functionality, do not configure 802.1ad NNI trunk ports and 802.1Q egress trunks with overlapping sets of allowed VLANs.
- Configuring nonisolated 802.1ad (C-UNI, S-UNI, NNI) internally uses interface port type NNI. Configuring isolated 802.1ad (C-UNI or S-UNI) without a Layer 2 protocol configuration internally uses interface port type ENI. Therefore, 802.1ad isolated and nonisolated port types (C-UNI, S-UNI, NNI) are mutually exclusive with interface port types (NNI, UNI, ENI).
- When configuring the service provider network for 802.1ad, be sure to configure 802.1ad NNIs on all interconnecting trunk ports. This is required for end-to-end functionality for customer Layer 2 PDUs in the service provider network.
- You cannot configure a port as an 802.1ad isolated C-UNI or S-UNI if an 802.1ad port type is already configured on an interface. The command is rejected with an error message.
- You cannot change the 802.1ad port type on an isolated C-UNI trunk port if VLAN mapping is configured on the port. You must remove the VLAN mapping configuration first.
- When you configure a port as an 802.1ad isolated or nonisolated S-UNI, this internally configures the switchport mode to dot1q-tunnel mode to provide port-based services. You are not allowed to change the switchport mode on an S-UNI.
- When you enter the **l2protocol forward** interface configuration command on an 802.1ad isolated UNI (S-UNI or C-UNI) to configure the BPDU action for Layer 2 protocols as *forward*, CDP and LLDP are disabled and STP BPDU filtering and Port Fast are enabled implicitly so that the provider edge switch does not participate in the customer topology.
- When you enter the **l2protocol peer** interface configuration command to configure the Layer 2 protocol action as *peer* for CDP, LLDP or STP, these protocols are automatically enabled on the isolated 802.1ad interface.
- When you remove an isolated or nonisolated 802.1ad configuration from a port, all implicit configuration is cleared from the interface except for platform port-type (UNI/ ENI/NNI).

- The sequence for saving 802.1ad and Layer 2 protocol commands has been changed in Cisco IOS release 12.2(55)SE so that **ethernet dot1ad** commands are saved in the startup configuration before **switchport** commands. This prevents any 802.1ad-related configuration from being lost if the system reloads or when a configuration is copied from a file to the running-configuration.

## Configuring 802.1ad EtherChannels

### 802.1ad EtherChannel Guidelines

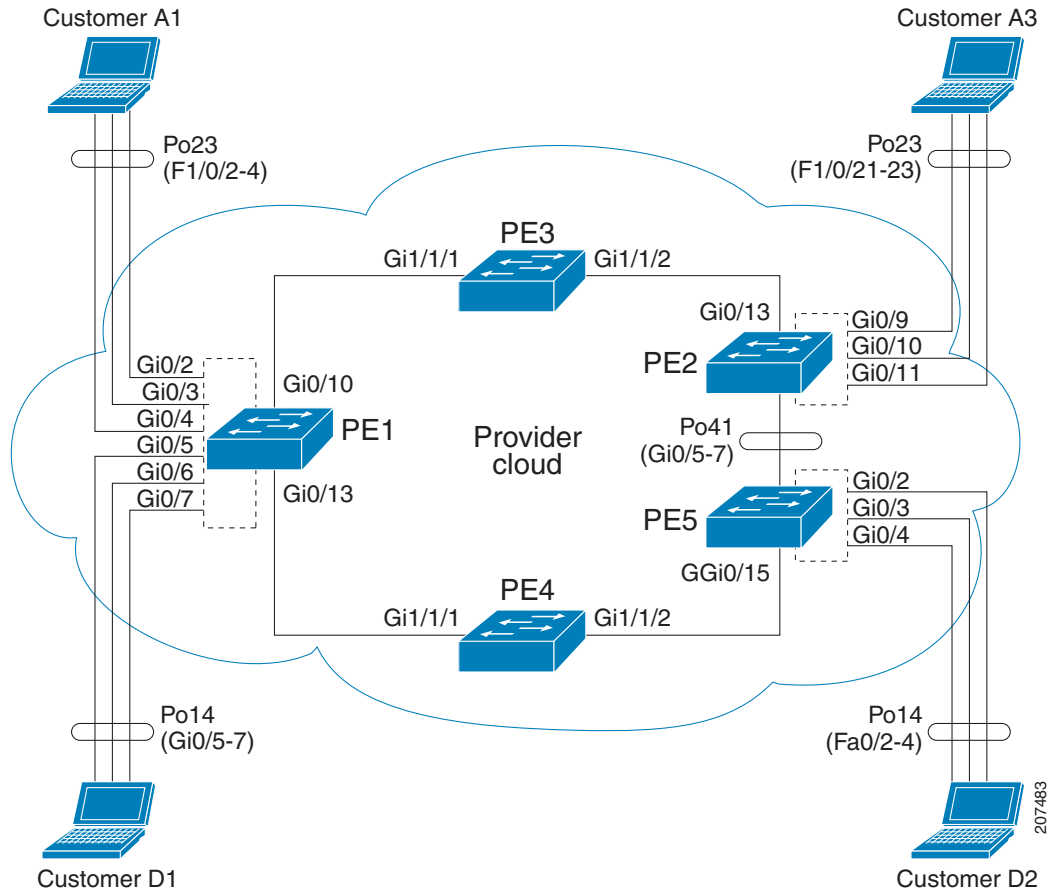
- When configuring isolated 802.1ad S-UNI or C-UNI on EtherChannels, configure the EtherChannel group first, and then configure 802.1ad port configuration on the EtherChannel interface. When configured on the EtherChannel port channel, the 802.1ad configuration is applied to all ports in the EtherChannel.
- For PAgP or LACP EtherChannels with isolated S-UNI or C-UNI, you must enter the **l2protocol peer pagp** or **l2protocol peer lacp** interface configuration command for the EtherChannel to function. Not entering these commands results in a continuous channel flap.
- When an EtherChannel is unbundled, all 802.1ad-implicit configuration is removed from the member ports of the EtherChannel. This includes STP, CDP, LLDP, and dot1q tunnel mode 802.1ad configuration. The configuration is not removed if the port is shut down.
- You cannot add a port to an EtherChannel if the port already has 802.1ad enabled.
- When you configure 802.1ad NNI or C-UNI on an EtherChannel port channel, before you add a new member port to the EtherChannel, you must configure switchport mode trunk on the new member. Failure to configure the new member as a trunk port results in a trunk encapsulation mismatch and the port is suspended.
- When you configure an 802.1ad C-UNI trunk port with VLAN mapping on an EtherChannel port channel, if you add a new member to the existing C-UNI EtherChannel, you must first configure trunk mode and VLAN mapping on the new member. Failure to configure these features results in a configuration mismatch between the EtherChannel and the new member port.
- When you apply a stored configuration that includes 802.1ad on a channel interface to a switch, you must make sure that the EtherChannel is formed first and the member ports are correctly configured before you apply the 802.1ad configuration. Directly applying a stored configuration to a switch can result in unexpected EtherChannel configuration, for example, ports not bundled into the EtherChannel, which could shut down the EtherChannel.

### \Configuration Example for 802.1ad End-to-End PAgP EtherChannels between CE Devices

Follow this configuration sequence when both CE and PE devices are actively participating in PAgP or LACP EtherChannels.

See [Figure 14-5](#). For end-to-end PAgP EtherChannel tunneling between CE devices, you should extend the CE connections through the service provider network as a point-to-point service when the PE device has no EtherChannels in **on** mode. See the [“Configuring Layer 2 Tunneling for EtherChannels”](#) section on [page 14-26](#). The same procedure applies to 802.1ad tunnels.

Figure 14-5 802.1ad End-to-End PAgP EtherChannels



Configuration on Customer A1

```
Switch #show etherchannel summary
```

```
Flags: D - down          P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3          S - Layer2
U - in use          f - failed to allocate aggregator
```

```
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
```

```
Number of channel-groups in use: 2
Number of aggregators:          2
```

Group	Port-channel	Protocol	Ports		
23	Po23 (SU)	PAgP (desirable)	Fa1/0/2 (P)	Fa1/0/3 (P)	Fa1/0/4 (P)



### Configuration on PE-1

#### UNI-S port mode

```
Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport mode access
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/3
Switch (config-if)# switchport mode access
Switch (config-if)# switchport access vlan 4001
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/4
Switch (config-if)# switchport mode access
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/10
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# ethernet dot1ad nni
```

#### UNI-C port mode

```
Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# switchport trunk allowed vlan 4002
Switch (config-if)# mapping default dot1ad-bundle 4002
Switch (config-if)# ethernet dot1ad uni c-port
```

Configuration on PE-2 is similar to PE-1

### Configuration on PE-3

```
Switch (config)# interface GigabitEthernet1/1/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# udd port aggressive
Switch (config-if)# ethernet dot1ad nni

Switch (config)# interface GigabitEthernet1/1/2
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# udd port aggressive
Switch (config-if)# ethernet dot1ad nni
Switch (config-if)# ethernet dot1ad nni
```

### Configuration on Customer A3

```
Switch (config)# interface Port-channel23
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk

Switch (config)# interface FastEthernet1/0/21
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable

Switch (config)# interface FastEthernet1/0/22
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
```

```
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable

Switch (config-if)# interface FastEthernet1/0/23
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable
```

### Configuration with 802.1ad C-UNI port on PE-2 and PE-3

```
Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4002
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4002
Switch (config-if)# Ethernet dot1ad uni c-port
```

```
Switch (config)# interface GigabitEthernet0/3
Switch (config-if)# switchport access vlan 4001
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4001
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4001
Switch (config-if)# Ethernet dot1ad uni c-port
```

```
Switch (config)# interface GigabitEthernet0/4
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4003
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4003
Switch (config-if)# Ethernet dot1ad uni c-port
```

The configuration on other switches remains the same in the 802.1ad C-UNI scenario.

## Configuring 802.1ad Split Horizon

Configuring the split-horizon feature on an 802.1ad C-UNI or S-UNI Layer 2 switchport maintains customer data confidentiality by preventing communication between customer-edge switches with the same VLAN IDs. Entering the **ethernet dot1ad uni {c-port isolate | s-port isolate}** interface configuration command on a port in the 802.1ad domain enables the split-horizon capability. By default, Layer 2 bridge protocol data units (BPDUs) are dropped on an 802.1ad isolated port.

You can set other actions (**forward** or **peer**) for specific protocols by entering the **l2protocol** interface configuration command on the isolated port and setting the action to be taken on the protocol packet. Entering **l2protocol forward** disables the protocol on the isolated port. When you enter **l2protocol peer**, if CDP, LLDP, or STP are configured on the peer, they are implicitly enabled on the isolated UNI port. You must enter other protocols and explicitly enable them on the isolated UNI port.

See this document for more information about IEEE 802.1ad support on Cisco provider bridges:

[http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce\\_cfm-ieee\\_802\\_1ad.html](http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_802_1ad.html)



### Note

As with other 802.1ad ports, an S-UNI isolated port must be an access port. A C-UNI isolated port can be either an access or a trunk port.

Beginning in privileged EXEC mode, follow these steps to configure split horizon on an 802.1ad port:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 3	<b>switchport mode access</b>	Configure the interface as an access port.
Step 4	<b>ethernet dot1ad uni {c- port isolate   s-port isolate}</b>	Configure the port for 802.1ad split horizon by enabling C-UNI or S-UNI port isolation. <ul style="list-style-type: none"> <li>• <b>c- port isolate</b>—Configure the port as a C-UNI isolated port.</li> <li>• <b>s-port isolate</b>—Configure the port as an S-UNI isolated port.</li> </ul> <p><b>Note</b> S-UNI isolated ports must be access ports. C-UNI isolated ports can be access or trunk ports.</p>
Step 5	<b>l2protocol [peer   forward] [protocol]</b>	(Optional) Configure the port to process or forward Layer 2 BPDUs. By default protocols are dropped on isolated C-UNIs and S-UNI s.
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>show ethernet dot1ad</b>	Verify the configuration.
Step 8	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable split horizon on an interface, enter the **no ethernet dot1ad uni {c- port isolate | s-port isolate}** interface configuration command.

This example configures an 802.1ad isolated UNI to drop all BPDUs:

```
Switch (config)# interface GigabitEthernet0/4
Switch (config-if)# switchport mode access
Switch (config-if)# ethernet dot1ad uni s-port isolate
Switch (config-if)# end
```

This example sets other actions to be taken on BPDUs on an 802.1ad isolated UNI by configuring the peer of the isolated UNI to process BPDUs.



**Note** Before you configure a port as an 802.1ad port, remove any Layer 2 protocol or VLAN mapping configuration from the port.

```
Switch (config)# interface GigabitEthernet0/4
Switch (config-if)# switchport mode access
Switch (config-if)# ethernet dot1ad uni s-port isolate
Switch (config-if)# l2protocol peer
Switch (config-if)# cdp enable
Switch (config-if)# lldp transmit
Switch (config-if)# lldp receive
Switch (config-if)# end
```

# Understanding Layer 2 Protocol Tunneling

Customers at different sites connected across a service-provider network need to use various Layer 2 protocols to scale their topologies to include all remote sites, as well as the local sites. STP must run properly, and every VLAN should build a proper spanning tree that includes the local site and all remote sites across the service-provider network. Cisco Discovery Protocol (CDP) must discover neighboring Cisco devices from local and remote sites. Link Layer Discovery Protocol (LLDP) advertises information about all devices, including non-Cisco devices, in the network. VLAN Trunking Protocol (VTP) must provide consistent VLAN configuration throughout all sites in the customer network.

**Note**

---

The Cisco ME switch does not support VTP; CDP, LLDP, and STP are supported by default on NNIs and can be enabled on ENIs. However, Layer 2 protocol tunneling is supported on all ports on the switch.

---

When protocol tunneling is enabled, edge switches on the inbound side of the service-provider network encapsulate Layer 2 protocol packets with a special MAC address and send them across the service-provider network. Core switches in the network do not process these packets but forward them as normal packets. Layer 2 protocol data units (PDUs) for CDP, LLDP, STP, or VTP cross the service-provider network and are delivered to customer switches on the outbound side of the service-provider network. Identical packets are received by all customer ports on the same VLANs with these results:

- Users on each of a customer's sites can properly run STP, and every VLAN can build a correct spanning tree based on parameters from all sites and not just from the local site.
- CDP discovers and shows information about the other Cisco devices connected through the service-provider network.
- LLDP discovers and shows information about the other devices, including non-Cisco devices, connected through the service-provider network.
- VTP provides consistent VLAN configuration throughout the customer network, propagating to all switches through the service provider that support VTP.

**Note**

---

To provide interoperability with third-party vendors, you can use the Layer 2 protocol-tunnel bypass feature. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling. You implement bypass mode by enabling Layer 2 protocol tunneling on the egress trunk port. When Layer 2 protocol tunneling is enabled on the trunk port, the encapsulated tunnel MAC address is removed and the protocol packets have their normal MAC address.

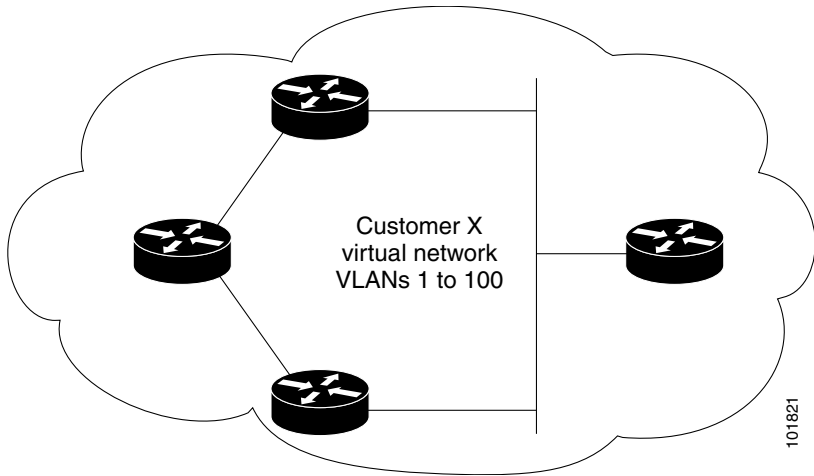
---

Layer 2 protocol tunneling can be used independently or can enhance 802.1Q tunneling. If protocol tunneling is not enabled on 802.1Q tunneling ports, remote switches at the receiving end of the service-provider network do not receive the PDUs and cannot properly run STP, CDP, and VTP. When protocol tunneling *is* enabled, Layer 2 protocols within each customer's network are totally separate from those running within the service-provider network. Customer switches on different sites that send traffic through the service-provider network with 802.1Q tunneling achieve complete knowledge of the customer's VLAN. If 802.1Q tunneling is not used, you can still enable Layer 2 protocol tunneling by connecting to the customer switch through access or trunk ports and enabling tunneling on the service-provider access or trunk port.

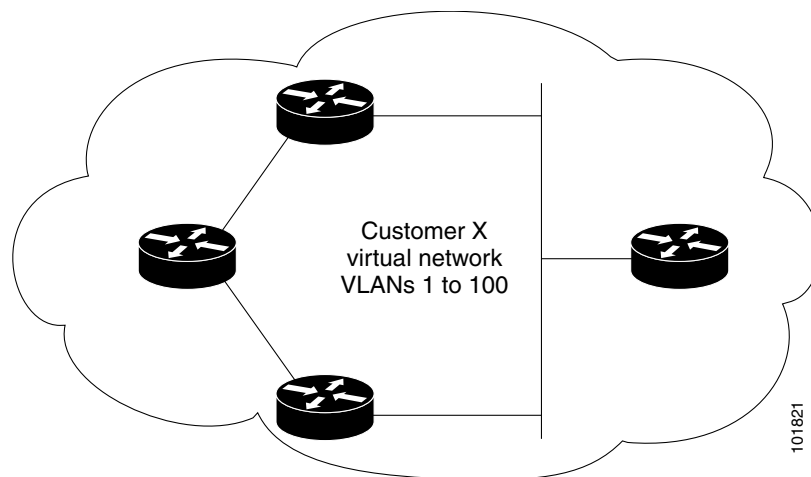
For example, in [Figure 14-6](#), Customer X has four switches in the same VLAN, that are connected through the service-provider network. If the network does not tunnel PDUs, switches on the far ends of the network cannot properly run STP, LLDP, CDP, and VTP. For example, STP for a VLAN on a switch in Customer X, Site 1, will build a spanning tree on the switches at that site without considering convergence parameters based on Customer X's switch in Site 2. This could result in the topology shown in [Figure 14-7](#).

**Figure 14-6** Layer 2 Protocol Tunneling

Customer X Site 1  
VLANs 1 to 100



**Figure 14-7** Layer 2 Network Topology without Proper Convergence



In an SP network, you can use Layer 2 protocol tunneling to enhance the creation of EtherChannels by emulating a point-to-point network topology. When you enable protocol tunneling (PAgP or LACP) on the SP switch, remote customer switches receive the PDUs and can negotiate the automatic creation of EtherChannels.

For example, in [Figure 14-8](#), Customer A has two switches in the same VLAN that are connected through the SP network. When the network tunnels PDUs, switches on the far ends of the network can negotiate the automatic creation of EtherChannels without needing dedicated lines. See the “[Configuring Layer 2 Tunneling for EtherChannels](#)” section on [page 14-26](#) for instructions.

**Figure 14-8** Layer 2 Protocol Tunneling for EtherChannels

## Configuring Layer 2 Protocol Tunneling

You can enable Layer 2 protocol tunneling (by protocol) on the ports that are connected to the customer in the edge switches of the service-provider network. The service-provider edge switches connected to the customer switch perform the tunneling process. Edge-switch tunnel ports are connected to customer 802.1Q trunk ports. Edge-switch access ports are connected to customer access ports. The edge switches connected to the customer switch perform the tunneling process.

You can enable Layer 2 protocol tunneling on ports that are configured as access ports, tunnel ports, or trunk ports. The switch supports Layer 2 protocol tunneling for CDP, LLDP, STP, and VTP. For emulated point-to-point network topologies, it also supports PAgP, LACP, and UDLD protocols.



### Caution

---

PAgP, LACP, and UDLD protocol tunneling is only intended to emulate a point-to-point topology. An erroneous configuration that sends tunneled packets to many ports could lead to a network failure.

---

When the Layer 2 PDUs that entered the service-provider inbound edge switch through a Layer 2 protocol-enabled port exit through the trunk port into the service-provider network, the switch overwrites the customer PDU-destination MAC address with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0). If 802.1Q tunneling is enabled, packets are also double-tagged; the outer tag is the customer metro tag, and the inner tag is the customer's VLAN tag. The core switches ignore the inner tags and forward the packet to all trunk ports in the same metro VLAN. The edge switches on the outbound side restore the proper Layer 2 protocol and MAC address information and forward the packets to all Layer 2 protocol-enabled access ports, tunnel ports, and trunk ports in the same metro VLAN. Therefore, the Layer 2 PDUs remain intact and are delivered across the service-provider infrastructure to the other side of the customer network.

See [Figure 14-6](#), with Customer X and Customer Y in access VLANs 30 and 40, respectively. Asymmetric links connect the customers in Site 1 to edge switches in the service-provider network. The Layer 2 PDUs (for example, BPDUs) coming into Switch B from Customer Y in Site 1 are forwarded to the infrastructure as double-tagged packets with the well-known MAC address as the destination MAC address. These double-tagged packets have the metro VLAN tag of 40, as well as an inner VLAN tag (for example, VLAN 100). When the double-tagged packets enter Switch D, the outer VLAN tag 40 is removed, the well-known MAC address is replaced with the respective Layer 2 protocol MAC address, and the packet is sent to Customer Y on Site 2 as a single-tagged frame in VLAN 100.

You can also enable Layer 2 protocol tunneling on access ports on the edge switch connected to access or trunk ports on the customer switch. In this case, the encapsulation and decapsulation process is the same as described in the previous paragraph, except that the packets are not double-tagged in the service-provider network. The single tag is the customer-specific access VLAN tag.

These sections contain this configuration information:

- [Default Layer 2 Protocol Tunneling Configuration, page 14-23](#)
- [Layer 2 Protocol Tunneling Configuration Guidelines, page 14-23](#)
- [Configuring Layer 2 Protocol Tunneling, page 14-25](#)
- [Configuring Layer 2 Tunneling for EtherChannels, page 14-26](#)

## Default Layer 2 Protocol Tunneling Configuration

[Table 14-1](#) shows the default Layer 2 protocol tunneling configuration.

**Table 14-1** *Default Layer 2 Ethernet Interface VLAN Configuration*

Feature	Default Setting
Layer 2 protocol tunneling	Disabled.
Shutdown threshold	None set.
Drop threshold	None set.
CoS value	If a CoS value is configured on the interface, that value is used to set the BPDU CoS value for Layer 2 protocol tunneling. If no CoS value is configured at the interface level, the default value for CoS marking of L2 protocol tunneling BPDUs is 5. This does not apply to data traffic.

## Layer 2 Protocol Tunneling Configuration Guidelines

- The switch supports tunneling of CDP, LLDP, STP including multiple STP (MSTP), and VTP. Protocol tunneling is disabled by default but can be enabled for the individual protocols on 802.1Q tunnel ports, access ports, or trunk ports.
- The edge switches on the outbound side of the service-provider network restore the proper Layer 2 protocol and MAC address information and forward the packets to all Layer 2 protocol-enabled tunnel, access, and trunk ports in the same metro VLAN.

- For interoperability with third-party vendor switches, the switch supports a Layer 2 protocol-tunnel bypass feature. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling. When Layer 2 protocol tunneling is enabled on ingress ports on a switch, egress trunk ports forward the tunneled packets with a special encapsulation. If you also enable Layer 2 protocol tunneling on the egress trunk port, this behavior is bypassed, and the switch forwards control PDUs without any processing or modification.
- The switch supports PAGP, LACP, and UDLD tunneling for emulated point-to-point network topologies. Protocol tunneling is disabled by default but can be enabled for the individual protocols on 802.1Q tunnel ports, access ports, or trunk ports.
- If you enable PAGP or LACP tunneling, we recommend that you also enable UDLD on the interface for faster link-failure detection.
- Loopback detection is not supported on Layer 2 protocol tunneling of PAGP, LACP, or UDLD packets.
- EtherChannel port groups are compatible with tunnel ports when the 802.1Q configuration is consistent within an EtherChannel port group.
- If an encapsulated PDU (with the proprietary destination MAC address) is received from a tunnel port or access or trunk port with Layer 2 tunneling enabled, the tunnel port is shut down to prevent loops. The port also shuts down when a configured shutdown threshold for the protocol is reached. You can manually re-enable the port (by entering a **shutdown** and a **no shutdown** command sequence). If errdisable recovery is enabled, the operation is retried after a specified time interval.
- Only decapsulated PDUs are forwarded to the customer network. The spanning-tree instance running on the service-provider network does not forward BPDUs to tunnel ports. CDP packets are not forwarded from tunnel ports.
- When protocol tunneling is enabled on an interface, you can set a per-protocol, per-port, shutdown threshold for the PDUs generated by the customer network. If the limit is exceeded, the port shuts down. You can also limit BPDU rate by using QoS ACLs and policy maps on a tunnel port.
- When protocol tunneling is enabled on an interface, you can set a per-protocol, per-port, drop threshold for the PDUs generated by the customer network. If the limit is exceeded, the port drops PDUs until the rate at which it receives them is below the drop threshold.
- Because tunneled PDUs (especially STP BPDUs) must be delivered to all remote sites so that the customer virtual network operates properly, you can give PDUs higher priority within the service-provider network than data packets received from the same tunnel port. By default, the PDUs use the same CoS value as data packets.
- Protocol tunneling for LLDP is supported beginning with Cisco IOS Release 12.2(58)SE.



## Configuring Layer 2 Protocol Tunneling

Beginning in privileged EXEC mode, follow these steps to configure a port for Layer 2 protocol tunneling:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and enter the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch. Valid interfaces can be physical interfaces and port-channel logical interfaces (port channels 1 to 48).
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	<b>switchport mode access</b> or <b>switchport mode dot1q-tunnel</b> or <b>switchport mode trunk</b>	Configure the interface as an access port, an 802.1Q tunnel port or a trunk port. The default switchport mode is access.
Step 5	<b>l2protocol-tunnel</b> [ <b>cdp</b>   <b>lldp</b>   <b>stp</b>   <b>vtp</b> ]	Enable protocol tunneling for the desired protocol. If no keyword is entered, tunneling is enabled for all three Layer 2 protocols.
Step 6	<b>l2protocol-tunnel shutdown-threshold</b> [ <b>cdp</b>   <b>lldp</b>   <b>stp</b>   <b>vtp</b> ] <i>value</i>	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface is disabled if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured.  <b>Note</b> If you also set a drop threshold on this interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.
Step 7	<b>l2protocol-tunnel drop-threshold</b> [ <b>cdp</b>   <b>lldp</b>   <b>stp</b>   <b>vtp</b> ] <i>value</i>	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface drops packets if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured.  If you also set a shutdown threshold on this interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.
Step 8	<b>exit</b>	Return to global configuration mode.
Step 9	<b>errdisable recovery cause l2ptguard</b>	(Optional) Configure the recovery mechanism from a Layer 2 maximum-rate error so that the interface is re-enabled and can try again. Errdisable recovery is disabled by default; when enabled, the default time interval is 300 seconds.
Step 10	<b>l2protocol-tunnel cos</b> <i>value</i>	(Optional) Configure the CoS value for all tunneled Layer 2 PDUs. The range is 0 to 7; the default is the default CoS value for the interface. If none is configured, the default is 5.
Step 11	<b>end</b>	Return to privileged EXEC mode.

	Command	Purpose
Step 12	<code>show l2protocol</code>	Display the Layer 2 tunnel ports on the switch, including the protocols configured, the thresholds, and the counters.
Step 13	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Use the `no l2protocol-tunnel [cdp | lldp | stp | vtp]` interface configuration command to disable protocol tunneling for one of the Layer 2 protocols or for all three of them. Use the `no l2protocol-tunnel shutdown-threshold [cdp | lldp | stp | vtp]` and the `no l2protocol-tunnel drop-threshold [cdp | lldp | stp | vtp]` commands to return the shutdown and drop thresholds to the default settings.

This example shows how to configure Layer 2 protocol tunneling for CDP, STP, and VTP and to verify the configuration.

```
Switch(config)# interface gigatEthernet0/1
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol
COS for Encapsulated Packets: 7
Port      Protocol Shutdown Drop      Encapsulation Decapsulation Drop
          Threshold Threshold Counter      Counter      Counter
-----
Gi 0/1   cdp      1500    1000 2288      2282      0
          stp      1500    1000 116       13        0
          vtp      1500    1000 3         67        0
          pagp    ----    ---- 0         0         0
          lacp    ----    ---- 0         0         0
          udld    ----    ---- 0         0         0
```


## Configuring Layer 2 Tunneling for EtherChannels

To configure Layer 2 point-to-point tunneling to facilitate the creation of EtherChannels, you need to configure both the SP edge switch and the customer switch.

### Configuring the SP Edge Switch

Beginning in privileged EXEC mode, follow these steps to configure a SP edge switch for Layer 2 protocol tunneling for EtherChannels:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface interface-id</code>	Enter interface configuration mode, and enter the interface to be configured as a tunnel port. This should be the edge port in the SP network that connects to the customer switch. Valid interfaces are physical interfaces.
Step 3	<code>no shutdown</code>	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	<code>switchport mode dot1q-tunnel</code>	Configure the interface as an 802.1Q tunnel port.

Command	Purpose
Step 5 <b>l2protocol-tunnel point-to-point</b> [pagp   lacp   udld]	(Optional) Enable point-to-point protocol tunneling for the desired protocol. If no keyword is entered, tunneling is enabled for all three protocols.   <b>Caution</b> To avoid a network failure, make sure that the network is a point-to-point topology before you enable tunneling for PAGP, LACP, or UDLD packets.
Step 6 <b>l2protocol-tunnel shutdown-threshold</b> [point-to-point [pagp   lacp   udld]] <i>value</i>	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface is disabled if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured.  <b>Note</b> If you also set a drop threshold on this interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.
Step 7 <b>l2protocol-tunnel drop-threshold</b> [point-to-point [pagp   lacp   udld]] <i>value</i>	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface drops packets if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured.  <b>Note</b> If you also set a shutdown threshold on this interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.
Step 8 <b>no cdp enable</b>	If the interface is an NNI, disable CDP on the interface. CDP is disabled by default on ENIs. UNIs do not support CDP.
Step 9 <b>spanning-tree bpdufilter enable</b>	If the interface is an NNI or ENI, enable BPDU filtering on the interface. UNIs do not support STP PBDU filtering.
Step 10 <b>exit</b>	Return to global configuration mode.
Step 11 <b>errdisable recovery cause l2ptguard</b>	(Optional) Configure the recovery mechanism from a Layer 2 maximum-rate error so that the interface is re-enabled and can try again. Errdisable recovery is disabled by default; when enabled, the default time interval is 300 seconds.
Step 12 <b>l2protocol-tunnel cos</b> <i>value</i>	(Optional) Configure the CoS value for all tunneled Layer 2 PDUs. The range is 0 to 7; the default is the default CoS value for the interface. If none is configured, the default is 5.
Step 13 <b>end</b>	Return to privileged EXEC mode.
Step 14 <b>show l2protocol</b>	Display the Layer 2 tunnel ports on the switch, including the protocols configured, the thresholds, and the counters.
Step 15 <b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no l2protocol-tunnel** [point-to-point [pagp | lacp | udld]] interface configuration command to disable point-to-point protocol tunneling for one of the Layer 2 protocols or for all three. Use the **no l2protocol-tunnel shutdown-threshold** [point-to-point [pagp | lacp | udld]] and the **no l2protocol-tunnel drop-threshold** [[point-to-point [pagp | lacp | udld]] commands to return the shutdown and drop thresholds to the default settings.

## Configuring the Customer Switch

After configuring the SP edge switch, begin in privileged EXEC mode and follow these steps to configure a customer switch for Layer 2 protocol tunneling for EtherChannels:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. This should be the customer switch port.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs and ENIs are disabled and NNIs are enabled.
Step 4	<b>switchport mode trunk</b>	Enable trunking on the interface.
Step 5	<b>udld enable</b>	Enable UDLD in <b>normal</b> mode on the interface.
Step 6	<b>channel-group</b> <i>channel-group-number</i> <b>mode desirable</b>	Assign the interface to a channel group, and specify <b>desirable</b> for the PAgP mode if the interface is an NNI or ENI. For more information about configuring EtherChannels, see <a href="#">Chapter 36, “Configuring EtherChannels and Link-State Tracking.”</a>
Step 7	<b>exit</b>	Return to global configuration mode.
Step 8	<b>interface port-channel</b> <i>port-channel number</i>	Enter port-channel interface mode.
Step 9	<b>shutdown</b>	Shut down the interface.
Step 10	<b>no shutdown</b>	Enable the interface.
Step 11	<b>end</b>	Return to privileged EXEC mode.
Step 12	<b>show l2protocol</b>	Display the Layer 2 tunnel ports on the switch, including the protocols configured, the thresholds, and the counters.
Step 13	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no switchport mode trunk**, the **no udld enable**, and the **no channel group channel-group-number mode desirable** interface configuration commands to return the interface to the default settings.

For EtherChannels, you need to configure both the SP edge switches and the customer switches for Layer 2 protocol tunneling. (See [Figure 14-8 on page 14-22.](#))

This example shows how to configure the SP edge switch 1 and edge switch 2. VLANs 17, 18, 19, and 20 are the access VLANs, Gigabit Ethernet interfaces 1 and 2 are point-to-point tunnel ports with PAgP and UDLD enabled, the drop threshold is 1000, and Fast Ethernet interface 3 is a trunk port.

SP edge switch 1 configuration:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport access vlan 17
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
```

```
Switch(config-if)# l2protocol-tunnel point-to-point uddl
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
```

SP edge switch 2 configuration:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point uddl
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point uddl
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
```

This example shows how to configure the customer switch at Site 1. Fast Ethernet interfaces 1, 2, 3, and 4 are set for 802.1Q trunking, UDLD is enabled, EtherChannel group 1 is enabled, and the port channel is shut down and then enabled to activate the EtherChannel configuration.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/4
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

# Monitoring and Maintaining Tunneling and Mapping Status

Table 14-2 shows the privileged EXEC commands for monitoring and maintaining 802.1Q and Layer 2 protocol tunneling and VLAN mapping.

**Table 14-2** Commands for Monitoring and Maintaining Tunneling

Command	Purpose
<b>clear l2protocol-tunnel counters</b>	Clear the protocol counters on Layer 2 protocol tunneling ports.
<b>show dot1q-tunnel</b>	Display 802.1Q tunnel ports on the switch.
<b>show dot1q-tunnel interface <i>interface-id</i></b>	Verify if a specific interface is a tunnel port.
<b>show interfaces [<i>interface interface-id</i>] vlan mapping</b>	Display VLAN mapping information for all interfaces or for the specified interface.
<b>show l2protocol-tunnel</b>	Display information about Layer 2 protocol tunneling ports.
<b>show errdisable recovery</b>	Verify if the recovery timer from a Layer 2 protocol-tunnel error disable state is enabled.
<b>show l2protocol-tunnel interface <i>interface-id</i></b>	Display information about a specific Layer 2 protocol tunneling port.
<b>show l2protocol-tunnel summary</b>	Display only Layer 2 protocol summary information.
<b>show platform vlan mapping</b>	Display platform VLAN mapping information.
<b>show vlan dot1q tag native</b>	Display the status of native VLAN tagging on the switch.
<b>show vlan mapping [<i>interface-id</i>]</b>	Display VLAN mapping information for all interfaces or for the specified interface.
<b>show vlan mapping usage</b>	Display information about hardware resource usage on the switch devoted to VLAN mapping.

For detailed information about these displays, see the command reference for this release.