



## CHAPTER 14

# Configuring IEEE 802.1Q Tunneling, VLAN Mapping, 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](#)
  - [Understanding Layer 2 Protocol Tunneling, page 14-12](#)
  - [Configuring Layer 2 Protocol Tunneling, page 14-15](#)
  - [Monitoring and Maintaining Tunneling and Mapping Status, page 14-23](#)

## 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.

all of the customer's VLANs. Configuring 802.1Q tunneling on a tunnel port is referred to as *traditional QinQ*

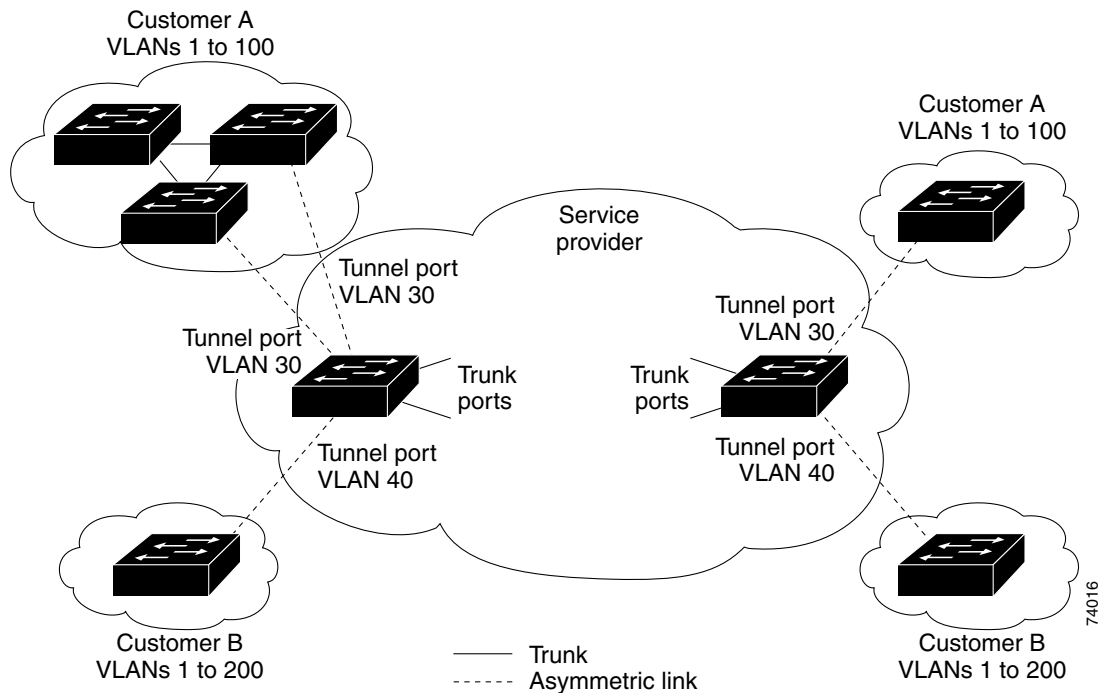
port, and the other end is configured as a tunnel port. You assign the tunnel port interface to an access VLAN ID that is unique to each customer. See [Figure 14-1](#).



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**

[Chapter 12, "Configuring VLANs."](#)

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

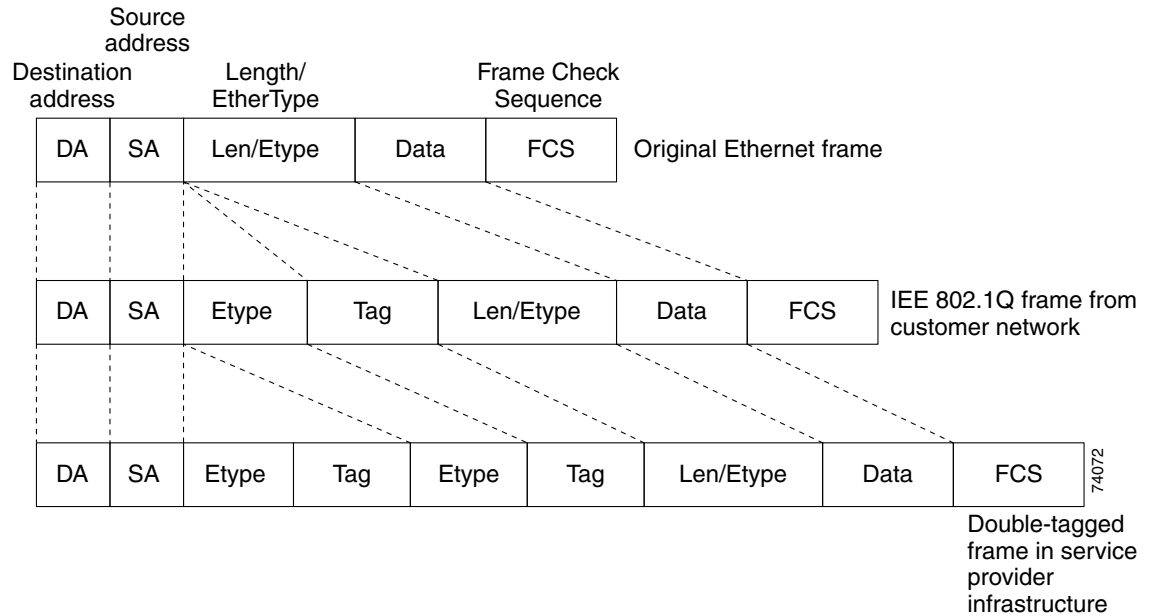


Packets coming from the customer trunk port into the tunnel port on the service-provider edge switch are normally 802.1Q-tagged with the appropriate VLAN ID. The the tagged packets remain intact inside the switch and when they exit the trunk port into the service-provider network, they are encapsulated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



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.

### Original (Normal), 802.1Q, and Double-Tagged Ethernet Packet Formats



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

- 
- [802.1Q Tunneling Configuration Guidelines, page 14-4](#)
- [802.1Q Tunneling and Other Features, page 14-5](#)  
[Configuring an 802.1Q Tunneling Port, page 14-6](#)

## Default 802.1Q Tunneling Configuration

## 802.1Q Tunneling Configuration Guidelines

### Native VLANs

. 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.

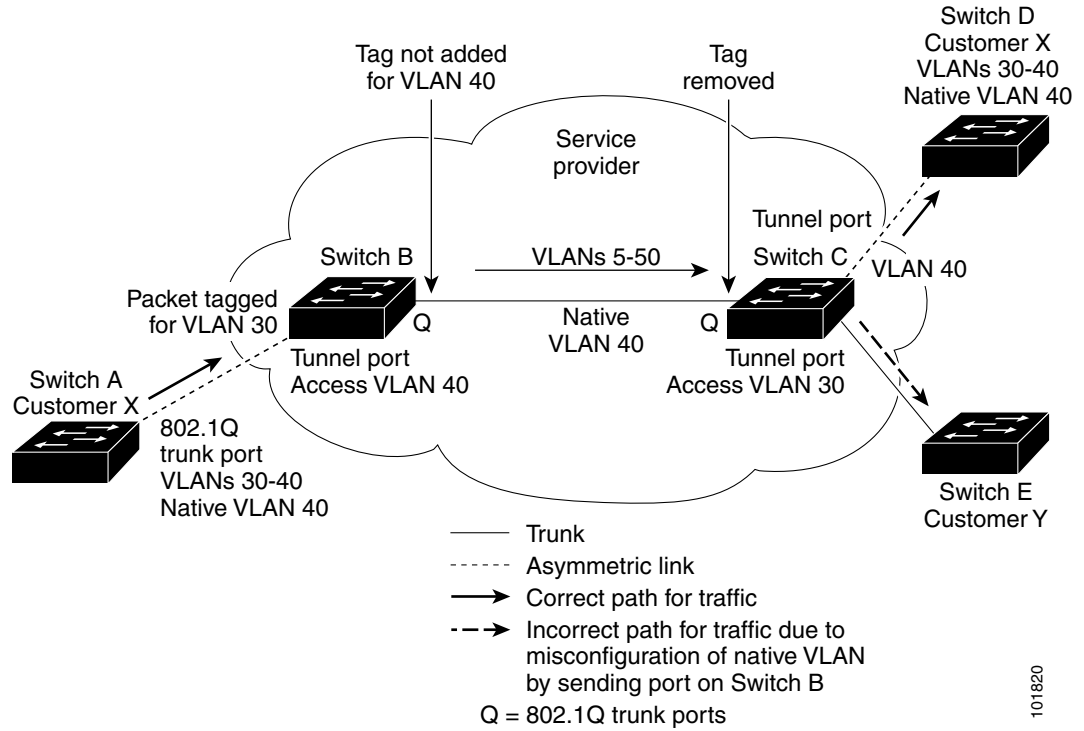
These are some ways to solve this problem:

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**

---

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



## System MTU

system mtu

system mtu

jumbo

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

  
Note

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

## Configuring an 802.1Q Tunneling Port

|        | Command                                      | Purpose |
|--------|--|---------|
| Step 1 | <b>configure terminal</b>                    |         |
| Step 2 | <i>interface-id</i>                          |         |
| Step 3 | <b>no shutdown</b>                           |         |
| Step 4 | <b>switchport access vlan</b> <i>vlan-id</i> |         |
| Step 5 |  |         |
| Step 6 | <b>exit</b>                                  |         |

|         | Command | Purpose |
|---------|---------|---------|
| Step 7  |         |         |
| Step 8  |         |         |
| Step 9  |         |         |
| Step 10 |         |         |
| Step 11 |         |         |

```
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
                exit
                vlan dot1q tag native
                end
                show dot1q-tunnel interface gigabitethernet0/2
dot1q-tunnel mode LAN Port(s)
-----
Gi0/1

Switch#
dot1q native vlan tagging is enabled
```

## Understanding VLAN Mapping



Note

---

---

- 
- 
- 



Note

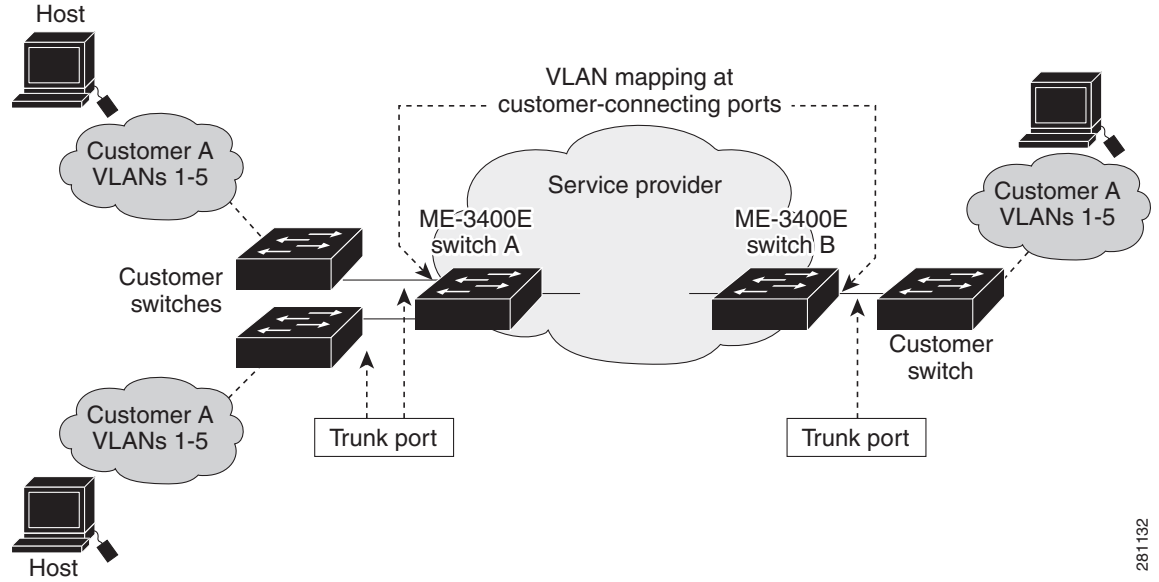
---

---

## Mapping Customer VLANs to Service-Provider VLANs



### Mapping Customer VLANs



281132

## One-to-One Mapping

|        | Command                        | Purpose  |
|--------|--------------------------------|--|
| Step 1 |                                |  |
| Step 2 | <i>interface-id</i>            |  |
| Step 3 | <b>switchport mode trunk</b>   |  |
|        | <b>switchport vlan mapping</b> | <p>—the customer VLAN ID (C-VLAN) entering the switch from the customer network. The range is from 1 to 4094.</p> <p>—the assigned service-provider VLAN ID (S-VLAN). The range is from 1 to 4094.</p> |
|        |                                | (Optional) Specify that all packets on the port are dropped if they do not match the VLANs specified in Step 4.  |
|        |                                | Return to privileged EXEC mode.  |
|        |                                | Verify the configuration.  |
|        |                                | (Optional) Save your entries in the configuration file.  |

*vlan-id translated-id*

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.

```
switchport vlan mapping 3 103
switchport vlan mapping 4 104
switchport vlan mapping 4 105
switchport vlan mapping default drop
exit
```

## Traditional QinQ on a Trunk Port

|        | Command | Purpose |
|--------|---------|---------|
| Step 1 |         |         |
| Step 2 |         |         |
| Step 3 |         |         |
| Step 4 |         |         |
| Step 5 |         |         |
| Step 6 |         |         |
| Step 7 |         |         |
| Step 8 |         |         |

```
switchport mode trunk
switchport trunk allowed 100
switchport vlan mapping default dot1q-tunnel 100
exit
```

## Selective QinQ on a Trunk Port

|        | Command | Purpose  |
|--------|---------|--|
| Step 1 |         |  |
| Step 2 |         |  |
| Step 3 |         |  |
| Step 4 |         | <ul style="list-style-type: none"> <li>•</li> <li>•</li> </ul> |
| Step 5 |         |  |
| Step 6 |         |  |
| Step 7 |         |  |
| Step 8 |         |  |

## Understanding Layer 2 Protocol Tunneling

**Note**

- 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.
- 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 14-5](#), 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, 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 14-6](#).

Figure 14-5 Layer 2 Protocol Tunneling

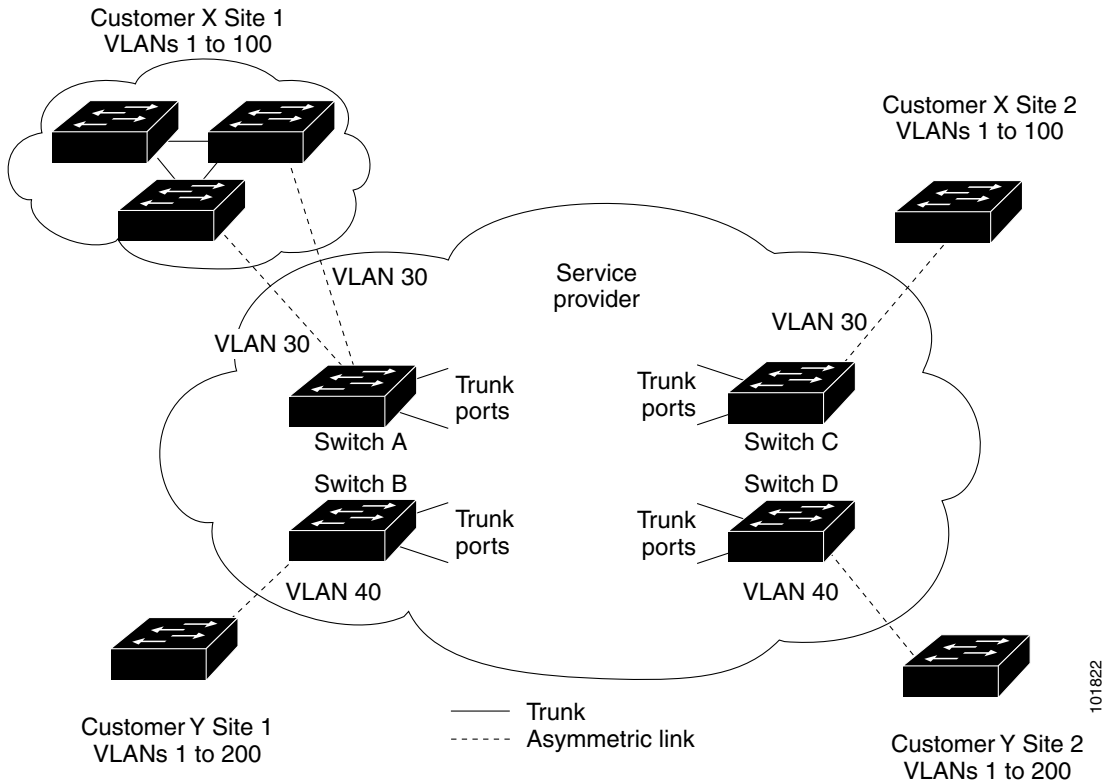
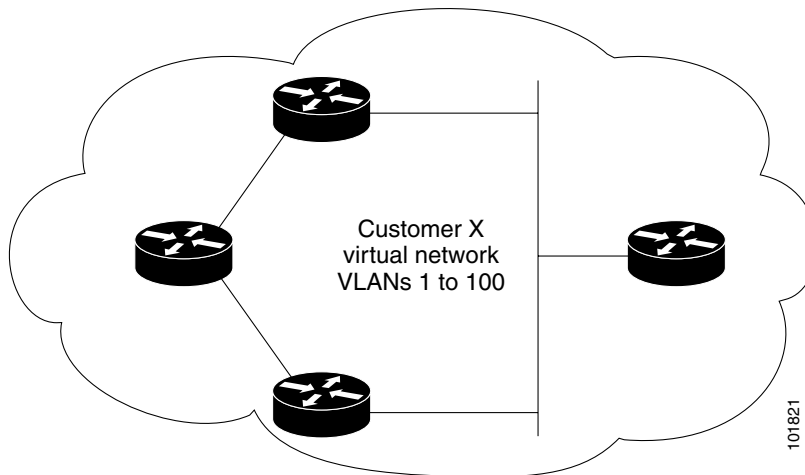
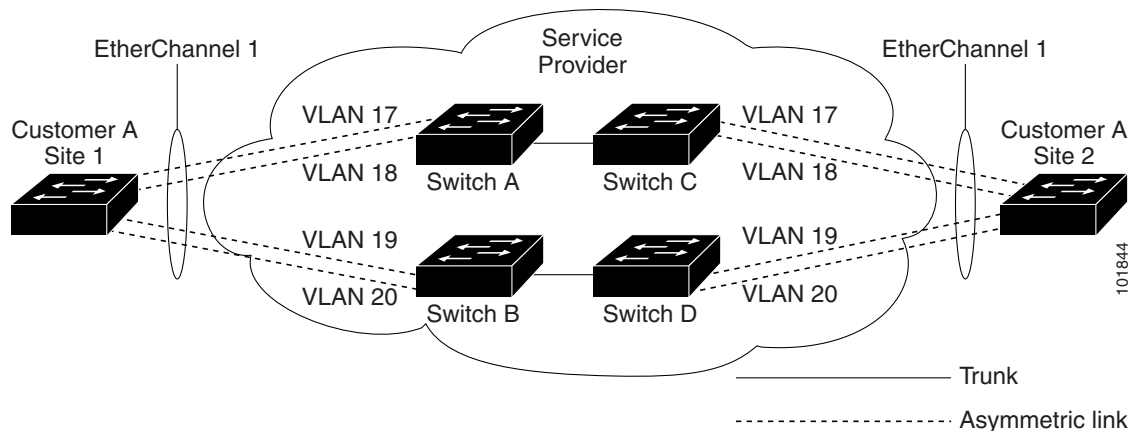


Figure 14-6 Layer 2 Network Topology without Proper Convergence



**Figure 14-7** *Layer 2 Protocol Tunneling for EtherChannels*



**Caution**

- 
- 
- 
- 

## Default Layer 2 Protocol Tunneling Configuration

*Default Layer 2 Ethernet Interface VLAN Configuration*

| Feature | Default Setting |
|---------|-----------------|
|         |                 |
|         |                 |
|         |                 |

## Layer 2 Protocol Tunneling Configuration Guidelines

- 
- 
-



- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

## Configuring Layer 2 Protocol Tunneling

|        | Command | Purpose |
|--------|---------|---------|
| Step 1 |         |         |
| Step 2 |         |         |
| Step 3 |         |         |

|   |  |
|---|--|
| or  | Configure the interface as an access port, an 802.1Q tunnel port or a trunk port. The default switchport mode is access.   |
| or  |  |
| <b>[cdp   stp   vtp]</b>                                      | Enable protocol tunneling for the desired protocol. If no keyword is entered, tunneling is enabled for all three Layer 2 protocols.  |
| <b>l2protocol-tunnel shutdown-threshold [cdp   stp   vtp]</b> | (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.<br><br>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.    |
| <b>l2protocol-tunnel drop-threshold [cdp   stp   vtp]</b>     | (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.<br><br>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. |
| <b>exit</b>   | Return to global configuration mode.   |
| <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.   |
| <b>l2protocol-tunnel cos</b>                                  | (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.  |
| <b>end</b>  | Return to privileged EXEC mode.  |
| <b>show l2protocol</b>  | Display the Layer 2 tunnel ports on the switch, including the protocols configured, the thresholds, and the counters.  |
| <b>copy running-config startup-config</b>                     | (Optional) Save your entries in the configuration file.  |

**no l2protocol-tunnel** [ **cdp** | **stp** | **vtp** ] interface configuration command to disable protocol tunneling for one of the Layer 2 protocols or for all three. Use the **shutdown-threshold** [ **cdp** | **stp** | **vtp** ] and the **drop-threshold** [ **cdp** | **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.


```

12protocol-tunnel cos 7
end
show 12protocol
COS for Encapsulated Packets: 7
Port      Protocol Shutdown Threshold Drop Threshold Encapsulation Counter Decapsulation Counter Drop 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
          udlid   ----      ----  0         0         0

```

## Configuring Layer 2 Tunneling for EtherChannels

### Configuring the SP Edge Switch

|        | Command | Purpose   |
|--------|---------|---|
| Step 1 |         |   |
| Step 2 |         |   |
| Step 3 |         |   |
| Step 4 |         |   |
| Step 5 |         |   |
|        |         | <br><b>Caution</b> |

|         | Command | Purpose     |
|---------|---------|-------------|
| Step 6  |         |             |
|         |         | <b>Note</b> |
| Step 7  |         |             |
|         |         | <b>Note</b> |
| Step 8  |         |             |
| Step 9  |         |             |
| Step 10 |         |             |
| Step 11 |         |             |
| Step 12 |         |             |
| Step 13 |         |             |
| Step 14 |         |             |
| Step 15 |         |             |



```
l2protocol-tunnel point-to-point udlld
l2protocol-tunnel drop-threshold point-to-point pagp 1000
exit
interface fastethernet0/3
no shutdown
switchport mode trunk

interface gigabitethernet0/1
switchport access vlan 19
switchport mode dot1q-tunnel
l2protocol-tunnel point-to-point pagp
l2protocol-tunnel point-to-point udlld
l2protocol-tunnel drop-threshold point-to-point pagp 1000
exit
interface gigabitethernet0/2
switchport access vlan 20
switchport mode dot1q-tunnel
l2protocol-tunnel point-to-point pagp
l2protocol-tunnel point-to-point udlld
l2protocol-tunnel drop-threshold point-to-point pagp 1000
exit
interface fastethernet0/3
no shutdown
switchport mode trunk

interface fastethernet0/1
no shutdown
switchport mode trunk
udld enable
channel-group 1 mode desirable
exit
interface fastethernet0/2
no shutdown
switchport mode trunk
udld enable
channel-group 1 mode desirable
exit
interface fastethernet0/3
no shutdown
switchport mode trunk
udld enable
channel-group 1 mode desirable
exit
interface fastethernet0/4
no shutdown
switchport mode trunk
udld enable
channel-group 1 mode desirable
exit
interface port-channel 1
shutdown
no shutdown
exit
```



