CHAPTER 8

# Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling

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 MWR 2941 router supports IEEE 802.1Q tunneling and Layer 2 protocol tunneling.

**Note** Release 15.0(1)MR does not support the 802.1ad standard.

**Note** For complete syntax and usage information for the commands used in this chapter, see the *Cisco MWR 2941 Mobile Wireless Edge Router IOS Command Reference, Release 15.0(1)MR*.



## Understanding 802.1Q Tunneling

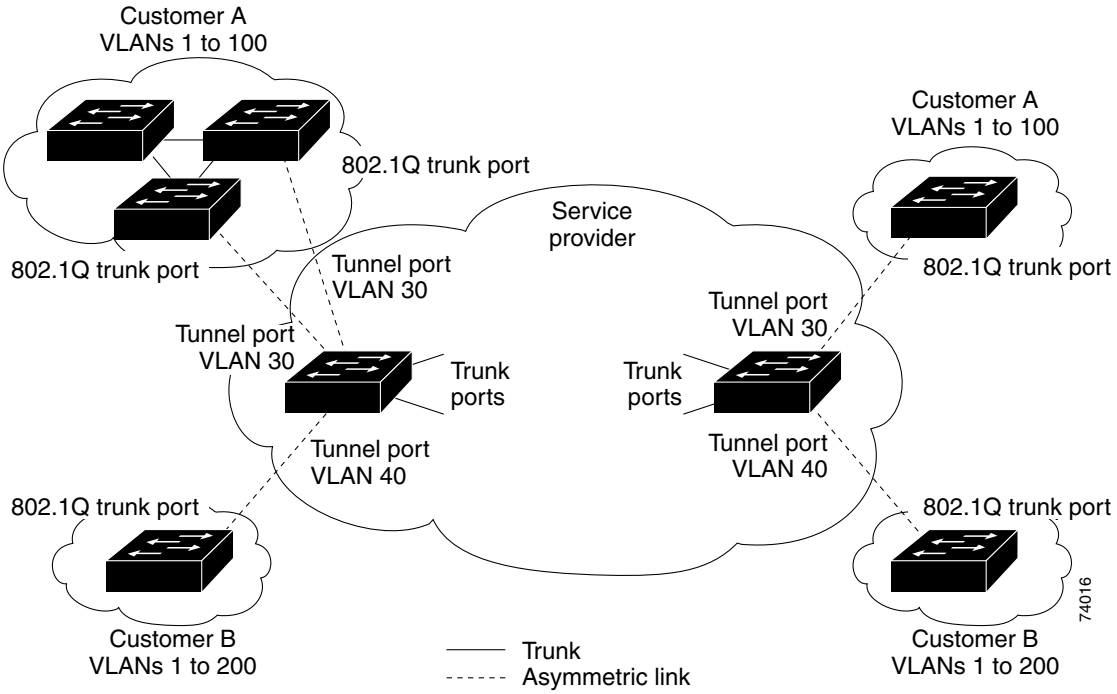
Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning 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 8-1.

***Figure 8-1 802.1Q Tunnel Ports in a Service-Provider Network***

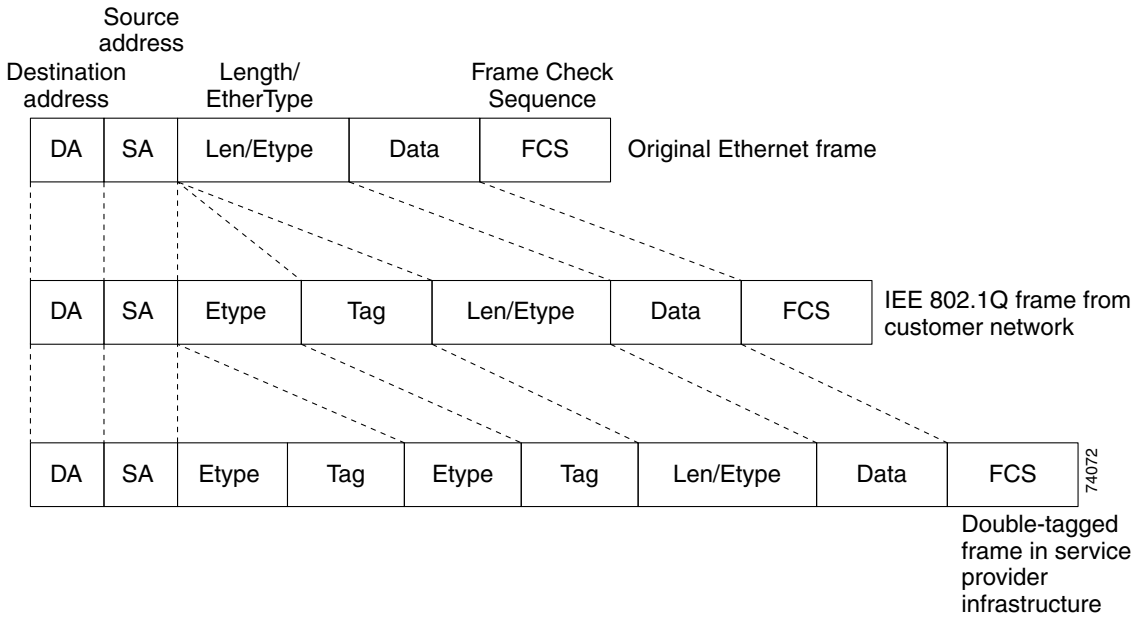



Packets coming from the customer trunk port into the tunnel port on the service-provider edge switch are normally 802.1Q-tagged with the appropriate VLAN ID. The the tagged packets remain intact inside the switch and when they exit the trunk port into the service-provider network, they are encapsulated 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 8-2 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 8-2 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 8-1, 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.

**Note** The Cisco MWR 2941 currently supports only one level of tagging.

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 match the CoS field of the inner tag (or customer tag) by default.

# Configuring 802.1Q Tunneling



## 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 router are dot1q tunnel ports.

## 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.

The following sections explain the configuration requirements for native VLANs and maximum transmission units (MTUs).

### 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 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 8-3. 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.

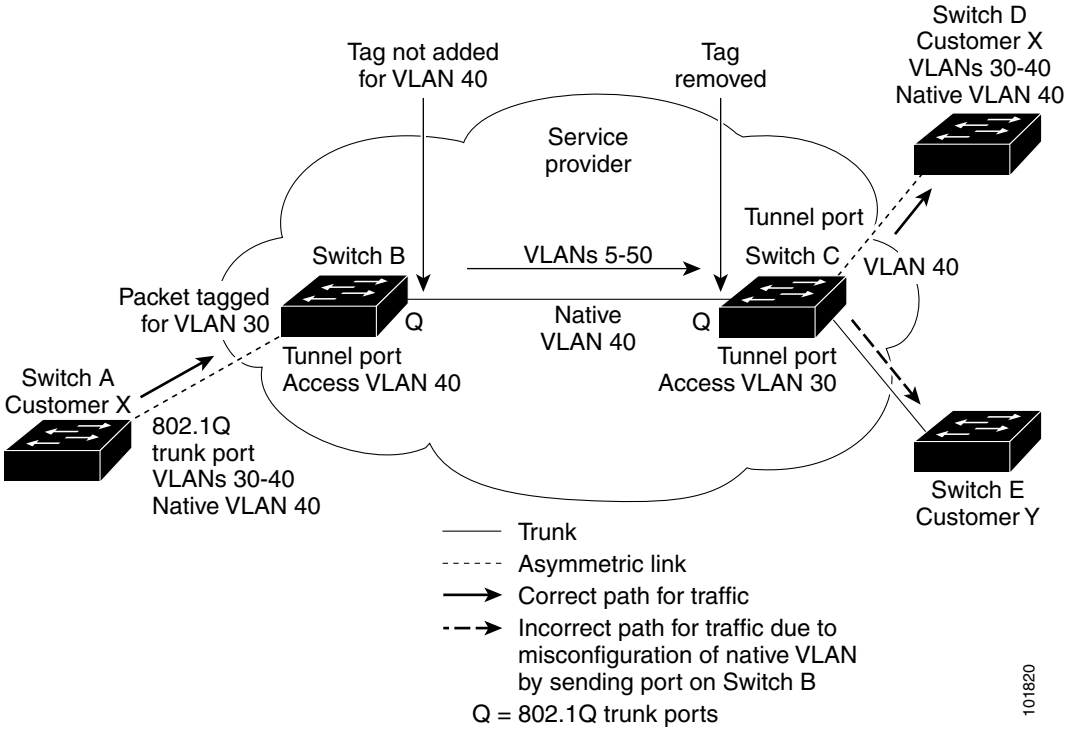
These are some ways to solve this problem:

- 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.

**Note** The Cisco MWR 2941 router 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 8-3 Potential Problem with 802.1Q Tunneling and Native VLANs***




## System MTU

The default MTU size for Gigabit Ethernet ports is 9216 bytes and is a fixed value. Release 15.0(1)MR does not support the **system mtu** or **system mtu jumbo** command.

# 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.

## Routing on VLANs with 802.1Q Tunnel Ports

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. The Cisco MWR 2941 does not support routing on switch virtual interfaces (SVIs).

# 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface** *interface-id* | 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. |
| **Step 3** | **no shutdown** | Enable the port, if necessary. NNIs are enabled by default. |
| **Step 4** | **switchport access vlan** *vlan-id* | Specify the default VLAN, which is used if the interface stops trunking. This VLAN ID is specific to the particular customer. |
| **Step 5** | **switchport mode dot1q-tunnel** | Set the interface as an 802.1Q tunnel port. |
| **Step 6** | **exit** | Return to global configuration mode. |
| **Step 7** | **vlan dot1q tag native** | (Optional) Set the router 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** | **end** | Return to privileged EXEC mode. |
| **Step 9** | **show running-config** | Display the ports configured for 802.1Q tunneling. |
| | **show dot1q-tunnel** | Display the ports that are in tunnel mode. |
| **Step 10** | **show vlan dot1q tag native** | Display 802.1Q native VLAN tagging status. |
| **Step 11** | **copy running-config startup-config** | (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.

```
Router(config)# interface gigabitethernet0/2
Router(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Router(config-if)# switchport mode dot1q-tunnel
```

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

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

There is no special configuration for provider trunk ports if the S-tags (outer VLAN tags) used in the provider network have a TPID of 0x8100, the TPID used in 802.1Q tags. The provider trunk ports are configured as normal trunk mode switch ports. If one of the other well known tunneling TPIDs is required the **dot1q tunneling ethertype tpid** interface configuration mode command is used to change it. Valid values for tpid are 0x88A8 (IEEE 802.1ad), 0x9100 and 0x9200. Use the **no** form of this command to set the TPID back to the default setting of 0x8100.

**Note** The Cisco MWR 2941 does not currently support IEEE 802.1ad.

# 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. Because the VLAN ID is mapped to the S-VLAN on ingress, all forwarding operations are performed based on S-VLAN information.

**Note** The Cisco MWR 2941 only supports VLAN mapping on 802.1q tunnel ports.

**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.

There are three types of VLAN mapping on 802.1q tunnel 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. The Cisco MWR 2941 does not currently support this type of VLAN mapping.
- Selective QinQ—Maps the specified customer VLANs entering the tunnel port to the specified S-VLAN ID. The S-VLAN is added to the incoming unmodified C-VLAN.

- 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 port as an 802.1Q tunnel port for traditional QinQ, or you can configure selective QinQ 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.

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

**Note** The Cisco MWR 2941 does not support one-to-one VLAN mapping.

**Note** The Cisco MWR 2941 does not currently support ingress classification and marking on dot1q interfaces.

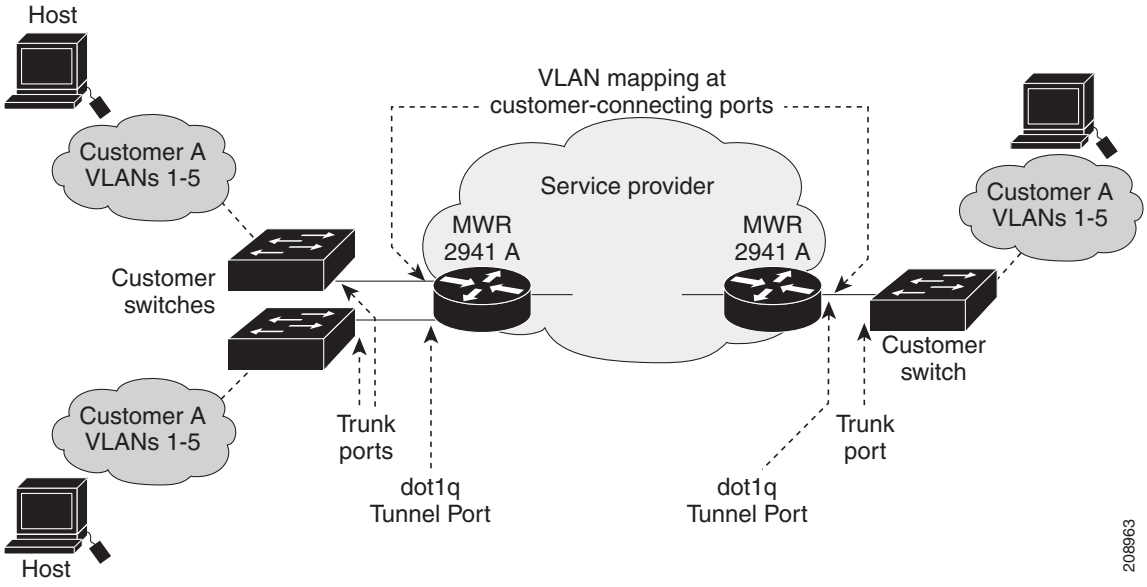
For information about Quality of Service, see the *Release Notes for Cisco MWR 2941 Mobile Wireless Edge Router for Cisco IOS Release 15.0(1)MR* and Chapter 24, "Configuring Quality of Service."

# Mapping Customer VLANs to Service-Provider VLANs

Figure 8-4 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 8-4 Mapping Customer VLANs***



# Configuring VLAN Mapping



## Default VLAN Mapping Configuration

By default, no VLAN mapping is configured.

## VLAN Mapping Configuration Guidelines

- The Cisco MWR 2941 uses 802.1Q tunnel ports for both traditional and selective QinQ. VLAN mapping is only supported on 802.1Q tunnel 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 **vlan dot1q tag native** 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 1 500** command, you should also enter the **vlan dot1q tag native** 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 running-config interface** privileged EXEC command with the **interface** *type number* keyword. See the "Monitoring and Maintaining Tunneling and Mapping Status" section on page 8-16 for the syntax of these commands. For more information about all commands in this section, see the *Cisco MWR 2941 Mobile Wireless Edge Router IOS Command Reference, Release 15.0(1)MR*.

### Configuring Traditional QinQ on an 802.1Q Tunnel Port

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

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **interface** *interface-id* | Enter interface configuration mode for the interface connected to the service-provider network. |
| Step 3 | **switchport mode dot1q-tunnel** | Configure the interface as a 802.1q tunnel port. |
| Step 4 | **switchport access vlan** *vlan-id* | Specify an outer VLAN ID to assign to all packets on the switch port. |
| Step 5 | **end** | Return to privileged EXEC mode. |

| | Command | Purpose |
|---|---|---|
| Step 6 | **show running-config interface** *type number* | Verify the configuration. |
| Step 7 | **copy running-config startup-config** | (Optional) Save your entries in the configuration file. |

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

```
Router(config)# interface gigabiethernet0/1
Router(config-if)# switchport mode dot1q-tunnel
Router(config-if)# switchport access vlan 100
Router(config-if)# exit
```

## Configuring Selective QinQ on a Tunnel 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.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **interface** *interface-id* | Enter interface configuration mode for the interface connected to the service-provider network. |
| Step 3 | **switchport mode dot1q-tunnel** | Configure the interface as a 802.1Q port. |
| Step 4 | **switchport vlan mapping** *original-vlan-id translated-vlan-id* | Enter the VLAN IDs to be mapped:<br>• *vlan-id*—the customer VLAN ID (C-VLAN) entering the router from the customer network. The range is from 1 to 4094. You can enter a string of VLAN-IDs.<br>• *outer-vlan-id*—Enter the outer VLAN ID (S-VLAN) of the service-provider network. The range is from 1 to 4094. |
| Step 5 | **end** | Return to privileged EXEC mode. |
| Step 6 | **show running-config interface** *type number* | Verify the configuration. |
| Step 7 | **copy running-config startup-config** | (Optional) Save your entries in the configuration file. |

Use the **no switchport vlan mapping** *vlan-id 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 router with an S-VLAN ID of 100. The traffic of any other VLAN IDs is tagged as VLAN 123.

```
Router(config)# interface gigabiethernet0/1
Router(config-if)# switchport mode dot1q-tunnel
Router(config-if)# switchport access vlan 123
Router(config-if)# switchport vlan mapping 1 100
Router(config-if)# switchport vlan mapping 2 100
Router(config-if)# switchport vlan mapping 3 100
Router(config-if)# switchport vlan mapping 4 100
Router(config-if)# switchport vlan mapping 5 100
```

```
Router(config-if)# exit
```

# 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. VLAN Trunking Protocol (VTP) must provide consistent VLAN configuration throughout all sites in the customer network that are participating in VTP.

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, 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.
- 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 8-5, 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 8-6.

*Figure 8-5 Layer 2 Protocol Tunneling*

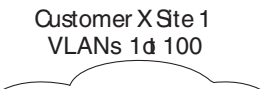
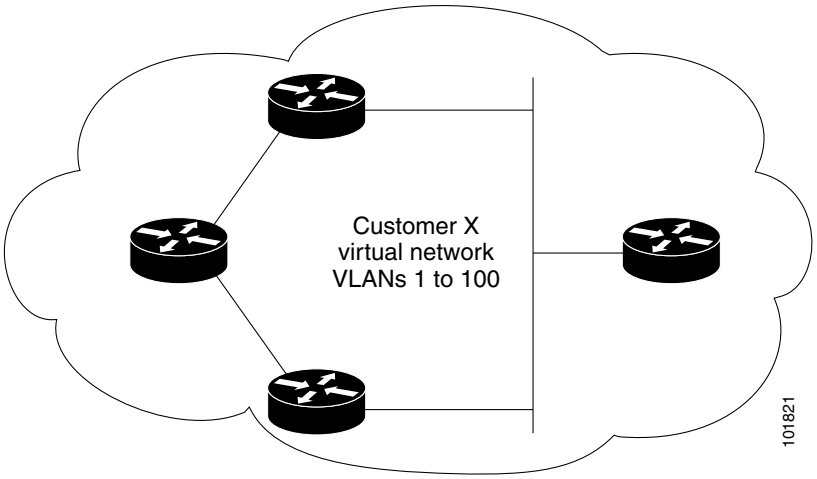



*Figure 8-6 Layer 2 Network Topology without Proper Convergence*



# 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, STP, and VTP. The switch does not support PAgP, LACP, and UDLD protocols for emulated point-to-point network topologies or Layer 2 protocol tunneling for LLDP.

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 8-5, 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

Table 8-1 shows the default Layer 2 protocol tunneling configuration.

*Table 8-1 Default Layer 2 Ethernet Interface VLAN Configuration*

| Feature | Default Setting |
|---|---|
| Layer 2 protocol tunneling | Disabled. |
| Shutdown threshold | None set. |

*Table 8-1 Default Layer 2 Ethernet Interface VLAN Configuration (continued)*

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

These are some configuration guidelines and operating characteristics of Layer 2 protocol tunneling:

- The router supports tunneling of CDP, 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.
- 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.

# 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 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **interface** *interface-id* | 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. |
| Step 3 | **no shutdown** | Enable the port, if necessary. NNIs are enabled by default. |
| Step 4 | **switchport mode access**<br>or<br>**switchport mode dot1q-tunnel**<br>or<br>**switchport mode trunk** | Configure the interface as an access port, an 802.1Q tunnel port or a trunk port. The default switchport mode is access. |
| Step 5 | **l2protocol-tunnel** [**cdp** \| **stp** \| **vtp**] | Enable protocol tunneling for the desired protocol. If no keyword is entered, tunneling is enabled for all three Layer 2 protocols. |
| Step 6 | **l2protocol-tunnel shutdown-threshold** [**cdp** \| **stp** \| **vtp**] *value* | (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>**Note** 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 | **l2protocol-tunnel drop-threshold** [**cdp** \| **stp** \| **vtp**] *value* | (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>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 | **exit** | Return to global configuration mode. |
| Step 9 | **errdisable recovery cause l2ptguard** | (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 | **l2protocol-tunnel cos** *value* | (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 | **end** | Return to privileged EXEC mode. |
| Step 12 | **show l2protocol** | Display the Layer 2 tunnel ports on the router, including the protocols configured, the thresholds, and the counters. |
| Step 13 | **copy running-config startup-config** | (Optional) Save your entries in the configuration file. |

Use the **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 **no l2protocol-tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] and the **no l2protocol-tunnel 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.

```
Router(config)# interface gigatethernet0/1
Router(config-if)# l2protocol-tunnel cdp
Router(config-if)# l2protocol-tunnel stp
Router(config-if)# l2protocol-tunnel vtp
Router(config-if)# l2protocol-tunnel shutdown-threshold 1500
Router(config-if)# l2protocol-tunnel drop-threshold 1000
Router(config-if)# exit
Router(config)# l2protocol-tunnel cos 7
Router(config)# end
Router# 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
```

# Monitoring and Maintaining Tunneling and Mapping Status

Table 8-2 shows the privileged EXEC commands for monitoring and maintaining 802.1Q and Layer 2 protocol tunneling and VLAN mapping.

*Table 8-2 Commands for Monitoring and Maintaining Tunneling*

| Command | Purpose |
|---|---|
| **clear l2protocol-tunnel counters** | Clear the protocol counters on Layer 2 protocol tunneling ports. |
| **show dot1q-tunnel** | Display 802.1Q tunnel ports on the router. |
| **show dot1q-tunnel interface** *interface-id* | Verify if a specific interface is a tunnel port. |
| **show running-config interface** *type number* | Verify the configuration for a specified interface. You can use this command to display the mapping configuration for a VLAN interface. |
| **show l2protocol-tunnel** | Display information about Layer 2 protocol tunneling ports. |
| **show errdisable recovery** | Verify if the recovery timer from a Layer 2 protocol-tunnel error disable state is enabled. |
| **show l2protocol-tunnel interface** *interface-id* | Display information about a specific Layer 2 protocol tunneling port. |
| **show l2protocol-tunnel summary** | Display only Layer 2 protocol summary information. |
| **show vlan dot1q tag native** | Display the status of native VLAN tagging on the router. |

For detailed information about these displays, see the *Cisco MWR 2941 Mobile Wireless Edge Router IOS Command Reference, Release 15.0(1)MR*.