Configuring Q-in-Q and Layer 2 Protocol Tunneling

This chapter describes how to configure IEEE 802.1Q-in-Q VLAN tunnels and Layer 2 protocol tunneling on the Cisco IR8340 Routers.

Information About Q-in-Q Tunnels

A Q-in-Q VLAN tunnel enables a service provider to segregate the traffic of different customers in their infrastructure, while still giving the customer a full range of VLANs for their internal use by adding a second 802.1Q tag to an already tagged frame.

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 the 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 of 4096 of the 802.1Q specification.

Using the 802.1Q tunneling feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved and the traffic from different customers is segregated within the service-provider infrastructure even when they appear to be on the same VLAN. The 802.1Q tunneling expands the VLAN space by using a VLAN-in-VLAN hierarchy and tagging 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 that is dedicated to tunneling. Each customer requires a separate VLAN, but that VLAN supports all of the customer's VLANs.

Customer traffic that is tagged in the normal way with appropriate VLAN IDs come 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 an asymmetric link 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.

Packets that enter the tunnel port on the service-provider edge switch, which are already 802.1Q-tagged with the appropriate VLAN IDs, are encapsulated with another layer of an 802.1Q tag that contains a VLAN ID that is unique to the customer. The original 802.1Q tag from the customer is preserved in the encapsulated packet. Therefore, packets that enter the service-provider infrastructure are double-tagged.

The outer tag contains the customer's access VLAN ID (as assigned by the service provider), and the inner VLAN ID is the VLAN of the incoming traffic (as assigned by the customer).

Information About Layer 2 Protocol Tunneling

Customers at different sites connected across a service-provider network need to run various Layer 2 protocols to scale their topology to include all remote sites, as well as the local sites. The Spanning Tree Protocol (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 infrastructure. The Cisco Discovery Protocol (CDP) must be able to discover neighboring Cisco devices from local and remote sites, and the VLAN Trunking Protocol (VTP) must provide consistent VLAN configuration throughout all sites in the customer network.

When protocol tunneling is enabled, edge switches on the inbound side of the service-provider infrastructure 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. Bridge protocol data units (BPDUs) for CDP, STP, or VTP cross the service-provider infrastructure 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.

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 BPDUs and cannot properly run STP, CDP, 802.1X, 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.

Note Layer 2 protocol tunneling works by tunneling BPDUs in the software. A large number of BPDUs that come into the supervisor will cause the CPU load to go up. You might need to make use of software rate limiters to reduce the load on the supervisor CPU. See Configuring Thresholds for Layer 2 Protocol Tunnel Ports, on page 5.

Configuring VLAN Mapping for Selective Q-in-Q on a 802.1Q Tunnel Port

To configure VLAN mapping for selective Q-in-Q on a 802.1Q tunnel port, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	[**no**] **vlan dot1q tag native** **Example:** `Router(config)# vlan dot1q tag native`	Enable or disable native VLAN tagging on trunk port.
Step 4	**interface** *interface-id* **Example:** `Router(config)# interface gigabitethernet 0/1/1`	Enters interface configuration mode for the interface connected to the service provider network.
Step 5	[**no**] **switchport mode dot1q-tunnel** **Example:** `Router(config-if)# switchport mode dot1q-tunnel`	Configure the interface as an IEEE 802.1Q tunnel port.
Step 6	[**no**] **switchport access vlan** *vlan id* **Example:** `Router(config-if)# switchport access vlan 20`	Configure default VLAN used as S-VLAN on dot1q-tunnel ports.
Step 7	[**no**] **switchport vlan mapping default dot1q-tunnel** *outer vlan-id*	Configure VLAN mapping so that all packets entering the port are bundled into the specified S-VLAN: • *outer vlan-id*—Enter the outer VLAN ID (S-VLAN) of the service provider network. The range is from 1 to 4094.
Step 8	[**no**] **switchport vlan mapping** *vlan-id* **dot1q-tunnel** *outer vlan-id*	Enters the VLAN IDs to be mapped: • *vlan-id*—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. • *outer vlan-id*—Enter the outer VLAN ID (S-VLAN) of the service provider network. The range is from 1 to 4094.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits the configuration mode.

Example

What to do next

Use the **no switchport vlan mapping all** command to remove the VLAN mapping configuration.

Enabling the Layer 2 Protocol Tunnel

You can enable protocol tunneling on the 802.1Q tunnel port.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface gigabitethernet 0/1/1`	Enters interface configuration mode.

Step 4	[**no**] **l2protocol-tunnel** [**cdp** | **vtp** | **stp**]
	Example:
	`Router(config-if)# l2protocol-tunnel stp`
	`Router(config-if)# no l2protocol-tunnel cdp`
		Enable or disable Layer 2 protocol tunneling. Optionally, you can enable CDP, STP, or VTP tunneling.

Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the configuration mode.

Configuring Thresholds for Layer 2 Protocol Tunnel Ports

You can specify the port drop and shutdown value for a Layer 2 protocol tunneling port.

When a drop threshold is enabled on a tunneling interface, the interface will drop any incoming PDU after the specified threshold for that protocol is reached. Similarly, when a shutdown threshold is enabled, the interface will be error-disabled when the threshold is exceeded. That effectively stops the interface from forwarding any packet. To enable the interface again, a user has to do 'shut' and 'no shut' to the interface. The unit of measure of both the thresholds is the number of packets per second. The valid range for configuration is between 1 to 4096. Both shutdown threshold and drop threshold can be enabled on a same interface for a same protocol. But shutdown threshold must be larger than drop threshold there.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface gigabitethernet 0/1/1`	Enters interface configuration mode.

Step 4	[**no**] **l2protocol-tunnel** {**drop-threshold** | **shutdown-threshold**} [**cdp** | **vtp** | **stp**] *packets-per-sec*
	Example:
	`Router(config-if)# l2protocol-tunnel shutdown-threshold stp 2000`
	`Router(config-if)# l2protocol-tunnel drop-threshold stp 2500`
	`Command rejected: protocol tunneling shutdown threshold must be greater than or equal to the drop threshold.`
	`Router(config-if)# l2protocol-tunnel drop-threshold stp 1500`
		drop-threshold—Specifies the maximum number of packets that can be processed on an interface before being dropped.
		shutdown-threshold—Specifies the maximum number of packets that can be processed on an interface. When the number of packets is exceeded, the port is put in error-disabled state.
		Optionally, you can specify CDP, STP, or VTP. Valid values for the packets are from 1 to 4096.
		Use the **no** form of the command to resets the threshold values to 0 and disable the shutdown threshold.

Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the configuration mode.

Verifying the Q-in-Q Configuration

Command	Purpose
show dot1q-tunnel	Display all ports in dot1q-tunnel mode.
show vlan mapping [*interface-id*]	Display the VLAN mapping information for all interfaces or for the interface specified.

VLAN Translation One-to-One Mapping

VLAN translation provides the capability of carrying the customers traffic in single tagged packets across the service provider network. Since VLAN translation and selective QinQ are applied to a trunk port, the service provider gets the added benefit of being able to selectively drop or bundle all traffic that does not belong to a given set of C-VLANs and bridge accordingly in the trunk.

VLAN translation on trunk ports supports 1:1 C-VLAN to S-VLAN mapping. C-VLAN received on customer side trunk port is stripped and mapped S-VLAN is added.

The SP provides L2VPN service to two different customers, Customer A and Customer B. The SP needs to keep the data as well as control traffic between the two customers separate from each other and also from the SP`s own control traffic. The SP network also needs to be transparent to the customer edge devices. Several mechanisms are available to keep the customer's VLAN ID space intact across the SP network.

IEEE802.1Q (Port-based QinQ) is one such mechanism wherein all the packets received on a *tunnel* port are tunneled through the SP network with the same outer tag. While such a mechanism is sufficient, it is rather restrictive and inflexible because it allows the SPs only port level granularity in providing the services.

The mechanisms described in the following sections and summarized in the following table give the SPs the ability to provide a more flexible and finer granular level of service. In all the following cases, the mappings of C-VLANs to S-VLANs at the ingress of the SP network and the correct mapping back from S-VLANs to C-VLANS at the egress of SP network relies on the proper configuration of the mappings and reverse mappings.

```
interface GigabitEthernet0/1/2
 switchport mode trunk
 switchport vlan mapping 10 100
 switchport vlan mapping 5 150

interface GigabitEthernet0/1/2
 switchport mode trunk
 switchport vlan mapping 10 dot1q-tunnel 100
 switchport vlan mapping 2-8 dot1q-tunnel 150
 switchport vlan mapping default dot1q-tunnel 300
```