Configuring Layer 2 Protocol Tunneling

This chapter describes how to configure Layer 2 protocol tunneling on the Cisco 7600 series routers.

Note

- For complete syntax and usage information for the commands used in this chapter, refer to the Cisco 7600 Series Routers Command References at this URL:

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- The WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6148-GE-TX, and WS-X6148V-GE-TX switching modules do not support Layer 2 protocol tunneling.

This chapter consists of these sections:

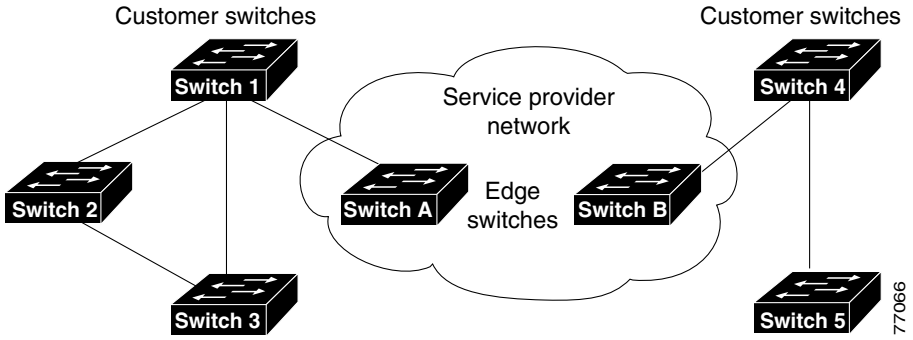
Understanding How Layer 2 Protocol Tunneling Works

Layer 2 protocol tunneling allows Layer 2 protocol data units (PDUs) (CDP, STP, and VTP) to be tunneled through a network. This section uses the following terminology:

- Edge router—The router connected to the customer router and placed on the boundary of the service provider network (see Figure 18-1).
- Layer 2 protocol tunnel port—A port on the edge router on which a specific tunneled protocol can be encapsulated or deencapsulated. The Layer 2 protocol tunnel port is configured through CLI commands.
- Tunneled PDU—A CDP, STP, or VTP PDU.

Without Layer 2 protocol tunneling, tunnel ports drop STP and VTP packets and process CDP packets. This handling of the PDUs creates different spanning tree domains (different spanning tree roots) for the customer switches. For example, STP for a VLAN on router 1 (see Figure 18-1) builds a spanning tree topology on switches 1, 2, and 3 without considering convergence parameters based on switches 4 and 5. To provide a single spanning tree domain for the customer, a generic scheme to tunnel BPDUs was created for control protocol PDUs (CDP, STP, and VTP). This process is referred to as Generic Bridge PDU Tunneling (GBPT).

Figure 18-1 Layer 2 Protocol Tunneling Network Configuration



GBPT provides a scalable approach to PDU tunneling by software encapsulating the PDUs in the ingress edge switches and then multicasting them in hardware. All switches inside the service provider network treat these encapsulated frames as data packets and forward them to the other end. The egress edge router listens for these special encapsulated frames and deencapsulates them; they are then forwarded out of the tunnel.

The encapsulation involves rewriting the destination media access control (MAC) address in the PDU. An ingress edge router rewrites the destination MAC address of the PDUs received on a Layer 2 tunnel port with the Cisco proprietary multicast address (01-00-0c-cd-cd-d0). The PDU is then flooded to the native VLAN of the Layer 2 tunnel port. If you enable Layer 2 protocol tunneling on a port, PDUs of an enabled protocol are not sent out. If you disable Layer 2 protocol tunneling on a port, the disabled protocols function the same way they were functioning before Layer 2 protocol tunneling was disabled on the port.

Configuring Support for Layer 2 Protocol Tunneling

Note

- Encapsulated PDUs received by an 802.1Q tunnel port are transmitted from other tunnel ports in the same VLAN on the router.
- Configure jumbo frame support on Layer 2 protocol tunneling ports:
  - See the "Configuring Jumbo Frame Support" section on page 8-8.
  - Take note of the modules listed in the "Configuring Jumbo Frame Support" section that do not support jumbo frames.

To configure Layer 2 protocol tunneling on a port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface` *type*[1] *slot/port*	Selects the LAN port to configure.
Step 2	`Router(config-if)# switchport`	Configures the LAN port for Layer 2 switching: • You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. • Required only if you have not entered the **switchport** command already for the interface.
Step 3	`Router(config-if)# l2protocol-tunnel [cdp|drop-threshold [`*packets*`|shutdown-threshold [`*packets*`]|stp|vtp]` `Router(config-if)# no l2protocol-tunnel [cdp|drop-threshold|shutdown-threshold|stp|vtp]`	Configures the Layer 2 port as a Layer 2 protocol tunnel port for the protocols specified. Clears the configuration.
Step 4	`Router(config)# end`	Exits configuration mode.
Step 5	`Router# show l2protocol-tunnel [interface` *type*[1] *slot/port*`|summary]`	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When you configure a Layer 2 port as a Layer 2 protocol tunnel port, note the following information:

- Optionally, you may specify a drop threshold for the port. The drop threshold value, from 1 to 4096, determines the number of packets to be processed for that protocol on that interface in one second. When the drop threshold is exceeded, PDUs for the specified protocol are dropped for the remainder of the 1-second period. If a shutdown threshold is not specified, the value is 0 (shutdown threshold disabled).
- Optionally, you may specify a shutdown threshold for the port. The shutdown threshold value, from 1 to 4096, determines the number of packets to be processed for that protocol on that interface in one second. When the shutdown threshold is exceeded, the port is put in errdisable state. If a shutdown threshold is not specified, the value is 0 (shutdown threshold disabled).

Note Refer to the *Cisco 7600 Series Router Cisco IOS Command Reference* for more information about the **l2ptguard** keyword for the following commands:

• errdisable detect cause

• errdisable recovery cause

This example shows how to configure Layer 2 protocol tunneling and shutdown thresholds on port 5/1 for CDP, STP, and VTP, and verify the configuration:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel shutdown-threshold cdp 10
Router(config-if)# l2protocol-tunnel shutdown-threshold stp 10
Router(config-if)# l2protocol-tunnel shutdown-threshold vtp 10
Router(config-if)# end
Router# show l2protocol-tunnel summary
```

```
Port   Protocol        Threshold
                       (cos/cdp/stp/vtp)
---------------------------------------
Fa5/1   cdp stp vtp     0/10  /10  /10          down trunk
Router#
```

This example shows how to display counter information for port 5/1:

```
Router# show l2protocol-tunnel interface fastethernet 5/1
Port   Protocol        Threshold           Counters
                       (cos/cdp/stp/vtp)   (cdp/stp/vtp/decap)
---------------------------------------------------------------
Router#
```

This example shows how to clear the Layer 2 protocol tunneling configuration from port 5/1:

```
Router(config-if)# no l2protocol-tunnel shutdown-threshold cdp 10
Router(config-if)# no l2protocol-tunnel shutdown-threshold stp 10
Router(config-if)# no l2protocol-tunnel shutdown-threshold vtp 10
Router(config-if)# no l2protocol-tunnel cdp
Router(config-if)# no l2protocol-tunnel stp
Router(config-if)# no l2protocol-tunnel vtp
Router(config-if)# end
Router# show l2protocol-tunnel summary
Port   Protocol        Threshold
                       (cos/cdp/stp/vtp)
---------------------------------------
Router#
```

This example shows how to clear Layer 2 protocol tunneling port counters:

```
Router# clear l2protocol-tunnel counters
Router#
```

Layer 2 Protocol Tunneling on EVC

Effective with Cisco IOS Release 15.3(1)S, the layer 2 protocol tunneling is supported on EVC. L2PT on EVC allows layer 2 PDUs (CDP, STP, and VTP) to be tunneled through an EVC. An ingress edge router rewrites the destination MAC address of the PDUs received on a layer 2 tunnel EVC with the Cisco proprietary multicast address (01-00-0c-cd-cd-d0). The PDU is then flooded to the bridge-domain VLAN of the layer 2 tunnel EVC port.

Restrictions for Layer 2 Protocol Tunneling on EVC

Following restrictions apply:

- Cisco IOS Release 15.3(1)S supports EVC on physical interfaces. Support on port-channel EVC will be introduced in the release 15.1(3)S1.
- Supports only CDP, VTP, MST (STP). Tagged protocols such as PVST and RPVST are not supported.
- Supported only on ES+ line cards.
- Only one customer per port is supported. This is because CDP, STP, and VTP are untagged, and it is not possible to distinguish packets from different customers.
- You can tunnel 1000 BPDUs per second without severely impacting the router performance.

- Configuration is allowed only on bridge domain.
- Configuration is allowed only on encapsulation default or encapsulation untagged.
- When **l2protocol tunnel** or **l2protocol tunnel stp** is configured, all the variants of STP BPDUs that ingress on the interface which has this service instance configured will be tunneled. Therefore, any features that rely on these BPDUs ingressing on this interface will not function. For instance, MST will not function for the service instances on this interface.
- You can specify (optional) a drop threshold globally using the **l2protocol-tunnel global drop-threshold** *pps* command. The drop threshold value(100-20000) determines the number of packets that should be processed for all the protocols configured on the switch. When the drop threshold exceeds, the PDUs for the protocols are dropped. This command impacts all the L2PT configurations on switch ports and EVC ports.

Note When the Layer 2 protocol tunneling EVC receives an encapsulated packet, it goes to error-disabled state and remains in that state. You should either manually enable the EVC or configure automatic recovery to bring the EVC status up. You can configure the automatic recovery timer using **errdisable recovery cause l2proto-tunnel** *time_value* command to automatically bring the EVC service instance status to up once the timer expires.

Configuring Layer 2 Protocol Tunneling on EVC

Complete these steps to configure L2PT on EVC:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot/port* or **interface tengigabitethernet** *slot/port*
4. **no ip address**
5. **service instance** *id* {**ethernet** [*service-name*]}
6. **encapsulation default**
   or
   encapsulation untagged
7. **l2protocol tunnel [cdp | stp | vtp]**
8. **bridge-domain** *bridge-id*
9. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* or **interface tengigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 6/1`	Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where: *slot/port*—Specifies the location of the interface.
Step 4	**no ip address** **Example:** `Router(config-if)# no ip address`	Disables IP processing on the interface.
Step 5	**service instance** *id* **{ethernet [***service-name***]}** **Example:** `Router(config-if)# service instance 100 ethernet`	Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the service instance submode.
Step 6	**encapsulation default** **or** **encapsulation untagged** **Example:** `Router(config-if-srv)# encapsulation default`	Configures the default service instance, or maps the untagged ingress ethernet frames on an interface.
Step 7	**l2protocol tunnel** [**cdp**|**stp**|**vtp**] **Example:** `Router(config-if-srv)#l2protocol tunnel stp`	Configures the EVC port as a Layer 2 protocol tunnel port for the protocols specified.

	Command	Purpose
Step 8	**bridge-domain bridge-id** **Example:** `Router(config-if-srv)#bridge-domain 200`	Binds the service instance to a bridge domain instance where *bridge-id* is the identifier for the bridge domain instance.
Step 9	**exit** **Example:** `Router(config-if-srv)# exit`	Exits the global service instance configuration mode.

Configuration Examples

This example shows the configuration on Switch A. See Figure 18-1:

```
Router# enable
Router# configure terminal
Router(config)# interface gigabitethernet 11/16
Router(config-if) no ip address
outer(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation default
Router(config-if-srv)# l2protocol tunnel cdp
Router(config-if-srv)# bridge-domain 100
```

This example shows the configuration on Switch B. See Figure 18-1:

```
Router# enable
Router# configure terminal
Router(config)# interface gigabitethernet 8/8
Router(config-if) no ip address
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation default
Router(config-if-srv)# l2protocol tunnel cdp
Router(config-if-srv)# bridge-domain 100
```

Verification

This example shows how to verify the configuration:

```
router#show ethernet service instance id 10 interface gigabitEthernet 8/8 detail
Service Instance ID: 10
Service Instance Type: static
Associated Interface: GigabitEthernet8/8
Associated EVC:
L2protocol tunnel cdp
CE-Vlans:
Encapsulation: default
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
   Pkts In   Bytes In    Pkts Out  Bytes Out
    169996   33999200     166967   33392595
EFP Microblocks:
***************
Microblock type: Bridge-domain
Bridge-domain: 100
```

This example shows the output on a line card:

```
router-dfc8#show ethernet service instance id 10 interface gigabitEthernet 11/16 detail
EFP ID: 100
Associated Interface: GigabitEthernet11/16
State: Up (redundancy state Up)
 Forwarding Service: Bridge Domain
L2protocol tunnel cdp
Encapsulation: default
Interface Dot1q Tunnel Ethertype: 0x8100

EFP Microblocks:
***************
Microblock type: Bridge-domain
Bridge-domain: 100
MAC security: Disabled
```

Troubleshooting Tips

Problem	Solution
How do I debug L2PT?	You can enable debugging from the Switch Processor (SP). Use these commands for debugging: **debug l2pt error**: Enables L2PT error debugs. **debug l2pt event:** Enables L2PT event debugs. **debug l2pt packet**: Enables L2PT packet information debugs.