Configuring Layer 1 and Layer 2 Features

This chapter provides information about configuring layer 1 and layer 2 features on the Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) line card on the Cisco 7600 series router. It includes the following topics:

- Cisco 7600 Synchronous Ethernet Support, page 4-2
- Configuring MultiPoint Bridging over Ethernet on Cisco 7600 Series ES+ Line Cards, page 4-32
- Backup Interface for Flexible UNI, page 4-38
- EVC on Port-Channel, page 4-48
- Configuring SPAN on EVC, page 4-53
- Configuring Layer 2 Access Control Lists (ACLs) on an EVC, page 4-66
- Configuring MST on EVC Bridge Domain, page 4-83
- Configuring Link State Tracking (LST), page 4-91
- MAC Address Security for EVC Bridge Domain, page 4-94
- CFM and PVST Co-Existence, page 4-111
- Custom Ethertype for EVC Interfaces, page 4-115
- Storm Control on Switchports and Ports Having EVCs, page 4-127
- Storm Control over EVC, page 4-135
- Asymmetric Carrier-Delay, page 4-138
- Manual Load Balancing for EVC over Port-Channel/LACP, page 4-140
- EVC Port Channel Per Flow Load Balancing, page 4-145
- Multichassis Support for LACP, page 4-150
- Pseudo MLACP Support on Cisco 7600, page 4-167
- Layer 2 Tunneling Protocol Version 3 (L2TPv3), page 4-178
- Reverse L2GP for Cisco 7600, page 4-183
- Configuring Resilient Ethernet Protocol, page 4-212
- IEEE 802.1ag-2007 Compliant CFM, page 4-237
- 802.1ah: Configuring the MAC Tunneling Protocol, page 4-276
- 802.3ah: Dying Gasp and Remote Loopback Initiation, page 4-285
Cisco 7600 Synchronous Ethernet Support

Synchronous Ethernet (SyncE) defined by the ITU-T standards such as G.8261 and G.8262 leverages the PHY layer of Ethernet to transmit clock information to the remote sites. SyncE over Ethernet provides a cost-effective alternative to the SONET networks. For SyncE to work, each network element along the synchronization path must support SyncE. To implement SyncE, the Bit clock of the Ethernet is aligned to a reliable clock traceable to Primary Reference Clock (PRC).

SyncE is implemented on an ES+ card for Cisco 7600 series routers. An ES+ card has a dedicated external interface known as BITS interface to recover clock from a Synchronization Supply Unit (SSU). The 7600 router uses this clock for SyncE. The BITS interface supports E1 (European SSUs) and T1 (American BITS) framing. Table 4-1 lists the framing modes for BITS port on an ES+ card:

<table>
<thead>
<tr>
<th>BITS/SSU port support Matrix</th>
<th>Framing modes supported</th>
<th>SSM/QL support</th>
<th>Tx Port</th>
<th>Rx Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>T1 ESF</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>T1</td>
<td>T1 SF</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>E1</td>
<td>E1 CRC4</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>E1</td>
<td>E1 FAS</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>E1</td>
<td>E1 CAS</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>


Note

The information provided in this chapter is applicable to both the ES+ and ES+T line cards unless specified otherwise.

Note

Follow these restrictions and guidelines while cross-bundling various line cards:
1. ES20 and ES+ cross-bundling is not supported.
2. Any LAN card, and ES20/ES+ cross-bundling is not supported.
<table>
<thead>
<tr>
<th>BITS/SSU port support Matrix</th>
<th>Framing modes supported</th>
<th>SSM/QL support</th>
<th>Tx Port</th>
<th>Rx Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>E1 CAS CRC4</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2048kHz</td>
<td>2048kHz</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 4-2 lists the External Timing Input and Output Pinouts:

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
<th>Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rx Ring</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Receive (Rx) Tip</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Not used</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Tx Ring</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Transmit (Tx) Tip</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Not used</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Not used</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Not used</td>
<td></td>
</tr>
</tbody>
</table>

Note
The pin out for BITS port on ES+ is similar to E1 and T1.

You can implement SyncE on an ES+ card with four different configurations:

- Clock Recovery from SyncE: System clock is recovered from the SyncE clocking source (gigabit and ten gigabit interfaces only). Router uses this clock as the Tx clock for other SyncE interfaces or ATM/CEoP interfaces.
- Clock Recovery from External Interface: System clock is recovered from a BITS clocking source.
- Line to External: The clock received from an Ethernet is forwarded to an external SSU. The SynE feature provides the functionality for clock cleanup. For a router in the middle of synchronization chain, the received clock may have unacceptable wander and jitter. The router recovers the clock from the SyncE interface, converts it to the format required for the BITS interface, and sends to a SSU through the BITS port. The SSU performs the cleanup and sends it back to the BITS interface. The cleaned up clock is received back from the SSU. This clock is used as Tx clock for the SyncE ports. For 7600 router, the interface from which the clock is recovered and the BITS port to the SSU should reside on the same ES+ card.
- System to External: The system clock is used as Tx clock for an external interface. By default the system clock is not transmitted on the external interface.

The SyncE enabled ES+ line card provides the squelching functionality, where an Alarm indication Signal (AIS) is sent to the Tx interfaces if the clock source goes down. The squelching functionality is implemented in two cases:

- Line to external: If the line source goes down, an AIS is transmitted on the external interface to the SSU.
- System to external: If the router loses all the clock sources, an AIS is sent on the external interface to the SSU.

Squelching is performed only towards an external device such as SSU or PRC.
You can have a maximum of six clock sources for a 7600 Router and a maximum of 4 clock sources on an ES+ card. The clock source with highest priority is made the default clock source. You can manage the clock sources on an ES+ card by changing the priority of the clock sources. You can also manage the synchronization on ES+ cards using the following management options:

- **Hold-off Time**: If a clock source goes down, the router waits for a specific hold-off time before removing the source. By default, the value of hold-off time is 300 ms.
- **Wait to Restore**: If a SyncE interface comes up, the router waits for a specific period of time before considering the SyncE interface for synchronization source. By default, the value is 300 sec.
- **Force Switch**: Forcefully select a synchronization source irrespective of whether the source is available or within the specified range.
- **Manual Switch**: Forcefully select a synchronization source provided the source is available and within the range.

### SSM and ESMC

Network Clocking uses these mechanisms to exchange the quality level of the clock between the network elements:

- **Synchronization Status Message**
- **Ethernet Synchronization Messaging Channel**

### Synchronization Status Message

Network elements use Synchronization Status Messages (SSM) to inform the neighboring elements about the Quality Level (QL) of the clock. The non-ethernet interfaces such as optical interfaces and SONET/T1/E1 SPA framers uses SSM. The key benefits of the SSM functionality:

- Prevents timing loops.
- Provides fast recovery when a part of the network fails.
- Ensures that a node derives timing from the most reliable clock source.

### Ethernet Synchronization Messaging Channel

In order to maintain a logical communication channel in synchronous network connections, ethernet relies on a channel called Ethernet Synchronization Messaging Channel (ESMC) based on IEEE 802.3 Organization Specific Slow Protocol standards. ESMC relays the SSM code that represents the quality level of the Ethernet Equipment Clock (EEC) in a physical layer.

The ESMC packets are received only for those ports configured as clock sources and transmitted on all the SyncE interfaces in the system. These packets are then processed by the Clock selection algorithm on RP and are used to select the best clock. The Tx frame is generated based on the QL value of the selected clock source and sent to all the enabled SyncE ports.

### Clock Selection Algorithm

Clock selection algorithm selects the best available synchronization source from the nominated sources. The clock selection algorithm has a non-revertive behavior among clock sources with same QL value and always selects the signal with the best QL value. For clock option 1, the default is revertive and for clock option 2, the default is non-revertive.
The clock selection process works in the QL enabled and QL disabled modes. When multiple selection processes are present in a network element, all processes work in the same mode.

**QL-enabled mode**

In QL-enabled mode, the following parameters contribute to the selection process:

- Quality level
- Signal fail via QL-FAILED
- Priority
- External commands.

If no external commands are active, the algorithm selects the reference (for clock selection) with the highest quality level that does not experience a signal fail condition. If multiple inputs have the same highest quality level, the input with the highest priority is selected. For multiple inputs having the same highest priority and quality level, the existing reference is maintained (if it belongs to this group), otherwise an arbitrary reference from this group is selected.

**QL-disabled mode**

In QL-disabled mode, the following parameters contribute to the selection process:

- Signal failure
- Priority
- External commands

If no external commands are active, the algorithm selects the reference (for clock selection) with the highest priority that does not experience a signal fail condition. For multiple inputs having the same highest priority, the existing reference is maintained (if it belongs to this group), otherwise an arbitrary reference from this group is selected.

**Hybrid mode**

The SyncE feature requires that each network element along the synchronization path needs to support SyncE. Timing over Packet (ToP) enables transfer of timing over an asynchronous network. The hybrid mode uses the clock derived from 1588 (PTP) to drive the system clock. This is achieved by configuring the Timing over Packet (ToP) interface on the PTP slave as the input source.

**Note**

The ToP interface does not support QL and works only in the QL-disabled mode.

The ES+ is a family of fixed-port SyncE line cards supporting 20 and 40 gbps bandwidth for the 7600 series routers. The following ES+ cards support SyncE:

- 4x10G XFP ports
- 40x1G SFP ports
- 2x10G XFP ports
- 20x1G SFP ports
- 4x10GE or 2x10GE with ITU-T G.709 DWDM optical interface

**Restrictions and Usage Guidelines**

Follow these restrictions and usage guidelines when configuring the SyncE on an ES40 line card:
If the network clock algorithm is enabled, all the ES+ cards on the router use the system clock as Tx clock (synchronous mode) for its ethernet interfaces. You cannot change the synchronous mode on a per interface basis for the line card. The whole line cards functions in the same mode.

On an ES+ card, you can have a maximum of 4 ports configured as clock source at a time.

For a 20x1 gigabit ES+ line card, you can select a maximum of two ports from each NPU.

For a 40x1 gigabit ES+ line card, you can select only one port from each NPU.

You can configure a maximum of 6 ports as a clock source for a Cisco 7600 router.

The line to external for clock clean up is supported only if the line interface and the external (BITS) interface are on the same ES+ line card.

SyncE feature is SSO co-existent, but not compliant. The clock selection algorithm is restarted on a switchover. During the switchover the router goes into hold-over mode.

The ES+ SyncE interfaces in WAN mode cannot be used for QL-enabled clock selection. You should either use them with the system in QL disabled mode or disable ESMC on the interfaces and use them as QL-disabled interfaces.

It is recommended that you do not configure multiple input sources with the same priority as this impacts the TSM switching delay.

You cannot implement the network-clock based clock selection algorithm and the new algorithm simultaneously. Both these algorithms are mutually exclusive.

SyncE is not supported on 1 Gigabit Ethernet copper SFPs (SFP GE-T and GLC-T).

Configuring Synchronous Ethernet on the Cisco 7600 Router with ES+ Line Card

This section describes how to configure SyncE for Cisco 7600 Router. SyncE is implemented on Cisco 7600 router using four different configurations:

- Configuring the Clock Recovery from SyncE, page 4-7
- Configuring the Clock Recovery from BITS Port, page 4-9
- Configuring the System to External, page 4-11
- Configuring the Line to External, page 4-12

Configuring the Clock Recovery from SyncE

This section describes how to configure SyncE over ES+ card on Cisco 7600 router using clock recovery from SyncE method.

SUMMARY STEPS

1. enable
2. configure terminal
3. network-clock synchronization automatic
4. network-clock synchronization ssm option option_Id Generation_Id
5. interface gigabitethernet slot/port or interface tengigabitethernet slot/port
6. [no]clock source {internal | line | loop}
7. synchronous mode
8. `exit`

9. `network-clock input-source priority {interface interface_name slot/card/port | {external slot/card/port }}`

10. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# enable</td>
</tr>
<tr>
<td>Enables privileged EXEC mode.</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>network-clock synchronization automatic</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# network-clock synchronization automatic</td>
</tr>
<tr>
<td>Enables the network clock selection algorithm. This command disables the Cisco specific network-clock process and turns on G.781 based automatic clock selection process.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>network-clock synchronization ssm option (option_id (GEN1</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# network-clock synchronization ssm option 2 GEN1</td>
</tr>
<tr>
<td>Configures the equipment to work in synchronization network. The option_id value 1 refers to synchronization networks design for Europe. This is the default value. The option_id value 2 refers to synchronization networks design for US.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>interface gigabitethernet slot/port or interface tengigabitethernet slot/port</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# int gig 5/1</td>
</tr>
<tr>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where: slot/port—Specifies the location of the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>clock source (internal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# clock source line</td>
</tr>
<tr>
<td>Indicates the clock source to use. The 3 options for clock source are:</td>
<td>• internal: Use internal clock.</td>
</tr>
<tr>
<td></td>
<td>• line: Recover clock from line.</td>
</tr>
<tr>
<td></td>
<td>• loop: Use local loop timing.</td>
</tr>
<tr>
<td>To implement SYNCE, use line option.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4      Configuring Layer 1 and Layer 2 Features

Cisco 7600 Synchronous Ethernet Support

Examples

This example shows how to configure clock recovery from SyncE for Cisco 7600 Routers:

```
Router> enable
Router# configure terminal
Router(config)# network-clock synchronization automatic
Router(config)# network-clock synchronization ssm option 2 GEN1
Router(config)# int gig 5/1
Router(config-if)# clock source line
Router(config-if)# synchronous mode
Router(config)# exit
Router(config)# network-clock input-source 1 interface TenGigabitEthernet7/1
Router(config)# exit
```

Configuring the Clock Recovery from BITS Port

This section describes how to configure SyncE over ES+ card on Cisco 7600 router using clock recovery from BITS port.

SUMMARY STEPS

1. enable
2. configure terminal
3. network-clock synchronization automatic
4. network-clock synchronization ssm option option_Id Generation_Id
5. network-clock input-source priority {interface interface_name slot/card/port | {external slot/card/port }}
6. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted.  
Example: Router# enable |
| **Step 2** configure terminal | Enters global configuration mode.  
Example: Router# configure terminal |
| **Step 3** network-clock synchronization automatic | Enables the network clock selection algorithm. This command disables the Cisco specific network-clock process and turns on G.781 based automatic clock selection process.  
Example: Router(config)# network-clock synchronization automatic |
| **Step 4** network-clock synchronization ssm option (option_id (GEN1 | GEN2)) | Configures the equipment to work in synchronization network. The option_id value 1 refers to synchronization networks design for Europe. This is the default value. The option_id value 2 refers to synchronization networks design for US.  
Example: Router(config)# network-clock synchronization ssm option 2 GEN1 |
| **Step 5** network-clock input-source priority {interface interface_name slot/card/port | {external slot/card/port }} | Enables clock recovery from BITS port.  
Example: Router(config-if-srv)# network-clock input-source 1 External 7/0/0 t1 sf |
| **Step 6** exit | Exits the global configuration mode  
Example: Router(config)# exit |
Examples

This example shows how to configure clock recovery from BITS port for Cisco 7600 Routers:

```
Router> enable
Router# configure terminal
Router(config)# network-clock synchronization automatic
Router(config)# network-clock synchronization ssm option 2 GEN1
Router(config)# network-clock input-source 1 External 7/0/0 t1 sf
Router(config)# exit
```

Configuring the System to External

This section describes how to configure SyncE over ES+ card on Cisco 7600 router using System to External method.

SUMMARY STEPS

1. enable
2. configure terminal
3. network-clock synchronization automatic
4. network-clock synchronization ssm option option_Id Generation_Id
5. network-clock output-source system priority { external slot/card/port [j1 | 2m | 10m] }
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>network-clock synchronization automatic</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# network-clock synchronization automatic</td>
</tr>
</tbody>
</table>
Cisco 7600 Synchronous Ethernet Support

Chapter 4 Configuring Layer 1 and Layer 2 Features

Cisco 7600 Synchronous Ethernet Support

Examples

This example shows how to configure system to external clocking for Cisco 7600 Routers:

```
Router> enable
Router# configure terminal
Router(config)# network-clock synchronization automatic
Router(config)# network-clock synchronization ssm option 2 GEN1
Router(config)# network-clock input-source 1 External 7/0/0 t1 sf
Router(config)# exit
```

This example shows how to configure clock clean-up using an SSU:

```
Router(config)# network-clock output-source line 1 interface GigabitEthernet1/11 External 1/0/0 t1 sf
Router(config)# network-clock input-source 1 External 7/0/0 t1 sf
```

Configuring the Line to External

This section describes how to configure SyncE over ES+ card on Cisco 7600 router using Line to External method.

SUMMARY STEPS

1. enable
2. configure terminal
3. network-clock synchronization automatic
4. network-clock synchronization ssm option option_Id Generation_Id

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>network-clock synchronization ssm option (option_id (GEN1</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# network-clock synchronization ssm option 2 GEN1</td>
</tr>
<tr>
<td>Step 5</td>
<td>network-clock output-source system priority (external slot/card/port [j1</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# network-clock output-source system 1 external 4/0/0 t1 sf</td>
</tr>
<tr>
<td>Step 6</td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>
5. `interface gigabitethernet slot/port` or `interface tengigabitethernet slot/port`

6. `[no]clock source {internal | line | loop}`

7. `synchronous mode`

8. `exit`

9. `network-clock output-source line priority {interface interface_name | controller {tl | e1} slot/card/port} | external slot/card/port}`

10. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><em>enable</em></td>
</tr>
<tr>
<td>Example:</td>
<td>Router# <code>enable</code></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Router# <code>configure terminal</code></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>network-clock synchronization automatic</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# <code>network-clock synchronization automatic</code></td>
</tr>
<tr>
<td></td>
<td>Enables the network clock selection algorithm. This command disables the Cisco specific network-clock process and turns on G.781 based automatic clock selection process.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`network-clock synchronization ssm option (option_id {GEN1</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# <code>network-clock synchronization ssm option 2 GEN1</code></td>
</tr>
<tr>
<td></td>
<td>Configures the equipment to work in synchronization network. The <code>option_id</code> value 1 refers to synchronization networks design for Europe. This is the default value. The <code>option_id</code> value 2 refers to synchronization networks design for US.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>interface gigabitethernet slot/port</code> or <code>interface tengigabitethernet slot/port</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# <code>int gig 5/1</code></td>
</tr>
<tr>
<td></td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where:</td>
</tr>
<tr>
<td></td>
<td>slot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>`clock source {internal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# <code>clock source line</code></td>
</tr>
<tr>
<td></td>
<td>Indicates the clock source to use. The 3 options for clock source are:</td>
</tr>
<tr>
<td></td>
<td>• internal: Use internal clock.</td>
</tr>
<tr>
<td></td>
<td>• line: Recover clock from line.</td>
</tr>
<tr>
<td></td>
<td>• loop: Use local loop timing.</td>
</tr>
<tr>
<td></td>
<td>To implement SYNCE, use <code>line</code> option.</td>
</tr>
</tbody>
</table>
Cisco 7600 Synchronous Ethernet Support

Chapter 4  Configuring Layer 1 and Layer 2 Features

Example:
This example shows how to configure clock recovery from SyncE for Cisco 7600 Routers:

```plaintext
Router> enable
Router# configure terminal
Router(config)# network-clock synchronization automatic
Router(config)# network-clock synchronization ssm option 2 GEN1
Router(config)# network-clock input-source 1 interface TenGigabitEthernet7/1
Router(config)# int gig 5/1
Router(config-if)# clock source line
Router(config-if)# synchronous mode
Router(config)# exit
Router(config)# network-clock output-source line 1 interface GigabitEthernet1/11 External 1/0/0
Router(config)# exit
```

Managing Synchronization on ES+ Card

Manage the synchronization on ES+ cards with these management commands:
• Quality Level Enabled Clock Selection: Use the `network-clock synchronization mode QL-enabled` command in global configuration mode to configure the automatic selection process for QL-enabled mode. This succeeds only if the SyncE interfaces are capable of sending SSM. The following example shows how to configure network clock synchronization (QL-enabled mode) in global configuration mode:

```bash
Router(config)# network-clock synchronization mode QL-enabled
```

• ESMC Process: Use the `esmc process` command in global configuration mode to enable the ESMC process at system level. The no form of the command disables the ESMC process. This command fails if there is no SyncE-capable interface installed in the platform. The following example shows how to enable ESMC in global configuration mode:

```bash
Router(config)# esmc process
```

• ESMC Mode: Use the `esmc mode [tx | rx |<cr>]` command in interface configuration mode to enable ESMC process at interface level. The no form of the command disables the ESMC process. The following example shows how to enable ESMC in interface configuration mode:

```bash
Router(config-if)# esmc mode tx
```

• Network Clock Source Quality level: Use the `network-clock source quality-level` command in interface configuration mode to configure the QL value for ESMC on gigabitethernet port. The value is based on global interworking options.

  - If Option 1 is configured, the available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.
  - If Option 2 is configured with GEN 2, the available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4 and QL-DUS.
  - If option 2 is configured with GEN1, the available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4 and QL-DUS

Use the `network-clock quality-level` command in global configuration mode to configure the QL value for SSM on BITS port. The following example shows how to configure `network-clock quality-level` in global configuration mode:

```bash
Router(config)# network-clock quality-level rx QL-PRC
```

The following example shows how to configure network-clock source quality-level in interface configuration mode:

```bash
Router(config-if)# network-clock source quality-level QL-PRC
```

• Wait-to-Restore: Use the `network-clock wait-to-restore timer global` command to set wait-to-restore time. You can configure the wait-to-restore time between 0 to 86400 seconds. The default value is 300 seconds. The wait-to-restore timer can be set at global configuration mode and interface configuration mode. The following example shows how to configure wait-to-restore timer in global configuration mode:

```bash
Router(config)# network-clock wait-to-restore 10 global
```

The following example shows how to configure the wait-to-restore timer in interface configuration mode:

```bash
Router(config)# int ten 7/1
Router(config-if)# network-clock wait-to-restore 10
```
- **Hold-off Time**: Use `network-clock hold-off timer global` command to configure hold-off time. You can configure the hold-off time to zero or any value between 50 to 10000 milliseconds. The default value is 300 milliseconds. The `network-clock hold-off timer` can be set at global configuration mode and interface configuration mode. The following example shows how to configure hold-off time:

  Router(config)# network-clock hold-off 50 global

- **Force Switch**: Use the `network-clock switch force` command to forcefully select a synchronization source irrespective of whether the source is available and within the range. The following example shows how to configure manual switch:

  Router(config)# network-clock switch force interface tenGigabitEthernet 7/1 t1

- **Manual Switch**: Use `network-clock switch manual` command to manually select a synchronization source provided the source is available and within the range. The following example shows how to configure manual switch:

  Router(config)# network-clock switch manual interface tenGigabitEthernet 7/1 t1

- **Clear Manual and Force Switch**: Use the `network-clock clear switch controller-id` command to clear the manual or switch it by force. The following example shows how to clear a switch:

  Router(config)# network-clock clear switch t0

- **Lock out a Source**: Use the `network-clock set lockout` command to lock-out a clock source. A clock source flagged as lock-out is not selected for SyncE. To clear the lock-out on a source, use the `network-clock clear lockout` command. The following example shows how to lock out a clock source:

  Router(config)# network-clock set lockout interface tenGigabitEthernet 7/1

  The following example shows how to clear lock-out on a clock source:

  Router(config)# network-clock clear lockout interface tenGigabitEthernet 7/1

### Verification

Use the following commands to verify the SyncE configuration:

- Use the `show network-clock synchronization` command to display the sample output:

  ```
  Router# show network-clocks synchronization
  Symbols:     En - Enable, Dis - Disable, Adis - Admin Disable
               NA - Not Applicable
               * - Synchronization source selected
               # - Synchronization source force selected
               & - Synchronization source manually switched
  
  Automatic selection process : Enable
  Equipment Clock : 2048 (EEC-Option1)
  Clock Mode : QL-Enable
  ESMC : Enabled
  SSM Option : 1
  T0 : TenGigabitEthernet12/1
  Hold-off (global) : 300 ms
  Wait-to-restore (global) : 300 sec
  Tsm Delay : 180 ms
  Revertive : No
  ```
Chapter 4  Configuring Layer 1 and Layer 2 Features

Cisco 7600 Synchronous Ethernet Support

Nominated Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>SigType</th>
<th>Mode/QL</th>
<th>Prio</th>
<th>QL_IN</th>
<th>ESMC Tx</th>
<th>ESMC Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>NA</td>
<td>NA/Dis</td>
<td>251</td>
<td>QL-SEC</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>*Te12/1</td>
<td>NA</td>
<td>Sync/En</td>
<td>1</td>
<td>QL-PRC</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>AT6/0/0</td>
<td>NA</td>
<td>NA/En</td>
<td>1</td>
<td>QL-SSU-A</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

- Use the `show network-clock synchronization detail` command to display all details of network-clock synchronization parameters at the global and interface levels.

Router# `show network-clocks synchronization detail`

Symbols:  En - Enable, Dis - Disable, Adis - Admin Disable
          NA - Not Applicable
          * - Synchronization source selected
          # - Synchronization source force selected
          & - Synchronization source manually switched

Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : TenGigabitEthernet12/1
Hold-off (global) : 300 ms
Wait-to-restore (global) : 300 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 2
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (sf_change)-> 1A (ql_change)-> 1A (sf_change)-> 1A
 (ql_change)-> 1A (ql_change)-> 1A (sf_change)-> 1A (ql_change)-> 1A
 (sf_change)-> 1A (ql_change)-> 1A

Nominated Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>SigType</th>
<th>Mode/QL</th>
<th>Prio</th>
<th>QL_IN</th>
<th>ESMC Tx</th>
<th>ESMC Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>NA</td>
<td>NA/Dis</td>
<td>251</td>
<td>QL-SEC</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>*Te12/1</td>
<td>NA</td>
<td>Sync/En</td>
<td>1</td>
<td>QL-PRC</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>AT6/0/0</td>
<td>NA</td>
<td>NA/En</td>
<td>1</td>
<td>QL-SSU-A</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

Interface:
---------------------------------------------
Local Interface: Internal
Signal Type: NA
Mode: NA(Ql-enabled)
SSM Tx: Disable
SSM Rx: Disable
Priority: 251
QL Receive: QL-SEC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 0
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE

Local Interface: Te12/1
Signal Type: NA
Mode: Synchronous (Ql-enabled)
ESMC Tx: Enable
ESMC Rx: Enable
Priority: 1
QL Receive: QL-PRC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: QL-DNU
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 300
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE

Local Interface: AT6/0/0
Signal Type: NA
Mode: NA (Ql-enabled)
SSM Tx: Enable
SSM Rx: Enable
Priority: 1
QL Receive: QL-SSU-A
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 300
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE

- Use the `show esmc` command to display the sample output.

Router# show esmc
Interface: TenGigabitEthernet12/1
  Administrative configurations:
    Mode: Synchronous
    ESMC TX: Enable
    ESMC RX: Enable
    QL TX: -
    QL RX: -
  Operational status:
    Port status: UP
    QL Receive: QL-PRC
    QL Transmit: QL-DNU
    QL rx overrided: -
    ESMC Information rate: 1 packet/second
    ESMC Expiry: 5 second

Interface: TenGigabitEthernet12/2
  Administrative configurations:
    Mode: Synchronous
    ESMC TX: Enable
    ESMC RX: Enable
    QL TX: -
    QL RX: -
  Operational status:
    Port status: UP
    QL Receive: QL-DNU
    QL Transmit: QL-DNU
    QL rx overrided: QL-DNU
Use the `show esmc detail` command to display all details of esmc parameters at the global and interface levels.

Router# show esmc detail
Interface: TenGigabitEthernet12/1
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
  ESMC RX: Enable
  QL TX: -
  QL RX: -
Operational status:
  Port status: UP
  QL Receive: QL-PRC
  QL Transmit: QL-DNU
  QL rx overridden: -
  ESMC Information rate: 1 packet/second
  ESMC Expiry: 5 second
  ESMC Tx Timer: Running
  ESMC Rx Timer: Running
  ESMC Tx interval count: 1
  ESMC INFO pkts in: 2195
  ESMC INFO pkts out: 6034
  ESMC EVENT pkts in: 1
  ESMC EVENT pkts out: 16

Interface: TenGigabitEthernet12/2
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
  ESMC RX: Enable
  QL TX: -
  QL RX: -
Operational status:
  Port status: UP
  QL Receive: QL-DNU
  QL Transmit: QL-DNU
  QL rx overridden: QL-DNU
  ESMC Information rate: 1 packet/second
  ESMC Expiry: 5 second
  ESMC Tx Timer: Running
  ESMC Rx Timer: Running
  ESMC Tx interval count: 1
  ESMC INFO pkts in: 0
  ESMC INFO pkts out: 2159
  ESMC EVENT pkts in: 0
  ESMC EVENT pkts out: 10

**Troubleshooting the Synchronous Ethernet configuration**

The following debug commands are available for troubleshooting the Synchronous Ethernet configuration on the Cisco 7600 ES+ Line Card:
Troubleshooting Scenarios

<table>
<thead>
<tr>
<th>Debug Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug platform ssm</code></td>
<td>Deports issues related to SSM such as Rx, Tx, QL values and so on.</td>
</tr>
<tr>
<td><code>debug platform network-clock</code></td>
<td>Deports issues related to network clock such as alarms, OOR, active-standby sources not selected correctly and so on.</td>
</tr>
<tr>
<td><code>debug esmc error</code></td>
<td>Verifies whether the ESMC packets are transmitted or received with proper quality level values.</td>
</tr>
<tr>
<td><code>debug esmc event</code></td>
<td></td>
</tr>
<tr>
<td><code>debug esmc packet [interface &lt;interface name&gt;]</code></td>
<td></td>
</tr>
<tr>
<td><code>debug esmc packet rx [interface &lt;interface name&gt;]</code></td>
<td></td>
</tr>
<tr>
<td><code>debug esmc packet tx [interface &lt;interface name&gt;]</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note**

Before you troubleshoot, ensure that all the network clock synchronization configurations are complete.

**Troubleshooting**

Table 4-3 provides the troubleshooting solutions for the synchronous ethernet feature.
Table 4-3  Troubleshooting Scenarios

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect clock limit set or disabled queue limit mode</td>
<td>• Verify that there are no alarms on the interfaces. Use the <code>show network-clock synchronization detail</code> RP command to confirm.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning</strong> We suggest you do not use these debug commands without TAC supervision.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>show network-clock synchronization</code> command to confirm if the system is in revertive mode or non-revertive mode and verify the non-revertive configurations as shown in this example:</td>
</tr>
<tr>
<td></td>
<td>RouterB#show network-clocks synchronization</td>
</tr>
<tr>
<td></td>
<td>Symbols:  En - Enable, Dis - Disable, Adis - Admin Disable, NA - Not Applicable</td>
</tr>
<tr>
<td></td>
<td>• Synchronization source selected  # - Synchronization source force selected  &amp; - Synchronization source manually switched</td>
</tr>
<tr>
<td></td>
<td>Automatic selection process : Enable  Equipment Clock : 1544 (EEC-Option2)  Clock Mode : QL-Enable  ESMC : Enabled  SSM Option : GEN1  T0 : POS3/1/0  Hold-off (global) : 300 ms  Wait-to-restore (global) : 0 sec  Tsm Delay : 180 ms  <strong>Revertive : Yes&lt;&lt;&lt;&lt;If it is non revertive then it will show NO here.</strong></td>
</tr>
<tr>
<td>Nominated Interfaces</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>SigType</td>
</tr>
<tr>
<td>Prio</td>
<td>QL_IN</td>
</tr>
<tr>
<td>Internal</td>
<td>NA</td>
</tr>
<tr>
<td>251</td>
<td>QL-ST3</td>
</tr>
<tr>
<td>SONET 3/0/0</td>
<td>NA</td>
</tr>
<tr>
<td>3</td>
<td>QL-ST3</td>
</tr>
<tr>
<td><strong>PO3/1/0</strong></td>
<td>NA</td>
</tr>
<tr>
<td>1</td>
<td>QL-ST3</td>
</tr>
<tr>
<td>SONET 2/3/0</td>
<td>NA</td>
</tr>
<tr>
<td>4</td>
<td>QL-ST3</td>
</tr>
<tr>
<td>Problem</td>
<td>Solution</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reproduce the current issue and collect the logs using the <strong>debug network-clock errors</strong>, <strong>debug network-clock event</strong>, and <strong>debug network-clock sm</strong> RP commands.</td>
<td><strong>Warning</strong> We suggest you do not use these debug commands without TAC supervision.</td>
</tr>
<tr>
<td>Contact Cisco technical support if the issue persists.</td>
<td></td>
</tr>
<tr>
<td>Incorrect quality level (QL) values when you use the <strong>show network-clock synchronization detail</strong> command.</td>
<td><strong>Warning</strong> We suggest you do not use these debug commands without TAC supervision.</td>
</tr>
<tr>
<td>Use the **network clock synchronization SSM (option 1</td>
<td>option 2)** command to confirm that there is no framing mismatch. Use the <strong>show run interface</strong> command to validate the framing for a specific interface. For the SSM option 1 framing should be SDH or E1 and for SSM option 2, it should be SONET or T1.</td>
</tr>
<tr>
<td>Reproduce the issue using the <strong>debug network-clock errors</strong>, <strong>debug network-clock event</strong> and <strong>debug platform ssm</strong> RP commands or enable the <strong>debug hw-module subslot</strong> command.</td>
<td><strong>Warning</strong> We suggest you do not use these debug commands without TAC supervision.</td>
</tr>
<tr>
<td>Error message “%NETCLK-6-SRC_UPD: Synchronization source SONET 2/3/0 status (Critical Alarms(OOR)) is posted to all selection process” displayed.</td>
<td><strong>Warning</strong> We suggest you do not use these debug commands without TAC supervision.</td>
</tr>
<tr>
<td>Interfaces with alarms or OOR cannot be the part of selection process even if it has higher queue limit or priority. Use the <strong>debug platform network-clock</strong> RP command to troubleshoot network clock issues.</td>
<td></td>
</tr>
<tr>
<td>Reproduce the issue using the <strong>debug platform network-clock</strong> command enabled in a route processor or enable the <strong>debug network-clock event</strong> and <strong>debug network-clock errors</strong> RP commands.</td>
<td><strong>Warning</strong> We suggest you do not use these debug commands without TAC supervision.</td>
</tr>
</tbody>
</table>
Flexible QinQ Mapping and Service Awareness

Flexible QinQ Mapping and Service Awareness allows service providers to offer triple-play services, residential Internet access from a DSLAM, and business Layer 2 and Layer 3 VPN by providing for termination of double-tagged dot1q frames onto a Layer 3 subinterface at the access node.

The access node connects to the DSLAM through the Cisco 7600 Series ES+ line cards. This provides a flexible way to identify the customer instance by its VLAN tags, and to map the customer instance to different services.

Flexible QinQ Mapping and Service Awareness on Cisco 7600 Series ES+ line cards is supported only through Ethernet Virtual Connection Services (EVCS) service instances.

EVCS uses the concepts of EVCs (Ethernet virtual circuits) and service instances. An EVC is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider to a customer. It embodies the different parameters on which the service is being offered. A service instance is the instantiation of an EVC on a given port on a given router.

Figure 4-1 shows a typical metro architecture where the access router facing the DSLAM provides VLAN translation (selective QinQ) and grooming functionality and where the service routers (SR) provide QinQ termination into a Layer 2 or Layer 3 service.

Flexible QinQ Mapping and Service Awareness on Cisco 7600 Series ES+ line cards provides the following functionality:

- VLAN connect with local significance (VLAN local switching)
  - Single tag Ethernet local switching where the received dot1q tag traffic from one port is cross-connected to another port by changing the tag. This is a 1-to-1 mapping service and there is no MAC learning involved.
Flexible QinQ Mapping and Service Awareness

Chapter 4 Configuring Layer 1 and Layer 2 Features

- Double tag Ethernet local switching where the received double tag traffic from one port is cross-connected to another port by changing both tags. The mapping to each double tag combination to the cross-connect is 1-to-1. There is no MAC learning involved.
- Hairpinning: It is a cross connect between two EFPS on the same port.

Note Connect service does not support identifying BPDU packets.

- Selective QinQ (1-to-2 translation)
  - Cross connect—Selective QinQ adds an outer tag to the received dot1q traffic and then tunnels it to the remote end with Layer 2 switching or EoMPLS.
- Double tag translation (2-to-2 translation) Layer 2 switching—Two received tagged frames are popped and two new tags are pushed.
- Double tag termination (2-to-1 tag translation)
  - Ethernet MultiPoint Bridging over Ethernet (MPBE)—The incoming double tag is uniquely mapped to a single dot1q tag that is then used to do MPBE.
  - Double tag MPBE—The ingress line uses double tags in the ingress packet to look up the bridging VLAN. The double tags are popped and the egress line card adds new double tags and sends the packet out.
  - Double tag routing—Same as regular dot1q tag routing except that double tags are used to identify the hidden VLAN.
- Local VLAN significance—VLAN tags are significant only to the port.
  For the Cisco 7600 Series ES+ line card, the subinterface gets a hidden VLAN (a VLAN that is not configured and is allocated internally) associated to the subinterface. The hidden VLAN number has no correlation with the encapsulation VLAN (the VLAN visible to the user or in the wire). Because the encapsulation is local to the port, you can have the same encapsulation VLAN in multiple ports.
- Scalable EoMPLS VC—Single tag packets are sent across the tunnel.
- QinQ policing and QoS
- Layer 2 protocol data unit (PDU) packet
  - Starting with Cisco IOS Release 15.4(2)S, when you use `connect` and `xconnect` command, the CDP, DTP, and VTP packets are forwarded transparently only if they are tagged. See Table 4-38 for more information.
  - With `bridge-domain` command, if the Layer 2 PDUs are tagged, packets are dropped by default; if the Layer 2 PDUs are untagged, packets are treated per the physical port configuration. (With an untagged service instance with `bridge-domain` command, the CPU stops the PDU depending on the configuration). When the feature is configured on the EFP, the BPDU is passed by the EFP to the feature which makes the decision accordingly.

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines when configuring Flexible QinQ Mapping and Service Awareness on the Cisco 7600 Series ES+ line cards:

- Service Scalability:
  - Service Instances per network processor: 8000
  - Service instances per Line Card: 16000
– Service instances per port channel: 8000. This is subject to the number of members per NP. This value would reduce by the factor of the member links per NP. If the member links are spread across NPs, then the maximum number of service instances per port channel is unchanged.

– Using TCAM entries: The number of TCAMs an EVC uses depends on the encapsulation configured on the TCAM as shown in the following examples.

**Example 1**
```
service instance 1 eth
encap dot1q 100
TCAMS used - 1
```

**Example 2**
```
service instance 1 eth
encap dot1q 200 second dot1q 300
TCAMs used - 1
```

**Example 3**
```
service instance 1 eth
encap dot1q 201, 202
TCAMs used - 2 (one for each encapsulation)
```

**Example 4**
```
service instance 1 eth
encap dot1q 20-40
TCAMs used - 4
```

First entry to match vlans 20-23
Second entry to match vlans 24-31
Third entry to match vlans 32-39
Fourth entry to match vlan 40

A range does not always mean multiple TCAMs as shown in this example where only one TCAM entry is used.

**Example 5**
```
service instance 1 ethernet
encap dot1q 8-15
service instance 2 ethernet
encap dot1q 2000 second-dot1q 96-127
```

TCAMs used per EVC: 1
– Service instances per router: 32,000
– Bridge-domains per router: 4,000
– Local switching: 16,000
– Xconnect: 16,000
– Subinterface: 2,000
– Number of service instance on a particular domain: 110 per NP

• QoS Scalability:
  – Service instances per router: 32,000
  – Bridge-domains: 4,000
- Local switching: 16,000
- Xconnect: 16,000
- Subinterface: 2,000

**QoS Scalability:**
- Shaping: Parent queue is 2,000 and child queue is 16,000
- Marking: Parent queue is 2,000 and child queue is 16,000
- Maximum number of child queues (leaf) supported for ES+T line card is 16 per port.

**Modular QoS CLI (MQC) actions supported include:**
- Shaping
- Bandwidth
- Two priority queues per policy
- The `set cos` command, `set cos-inner` command, `set cos cos-inner` command, and `set cos-inner cos` command
- WRED aggregate
- Queue-limit

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface gigabitethernet slot/port` or `interface tengigabitethernet slot/port`
4. `service instance id ethernet [service-name]`
5. `encapsulation dot1q vlan-id`
6. `rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad dot1q vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | symmetric

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
</tbody>
</table>
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 3    | `interface gigabitethernet slot/port` or `interface tengigabitethernet slot/port` | Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where:  
- `slot/port`—Specifies the location of the interface. |
| 4    | `service instance id ethernet [service-name]` | Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode. |
| 5    | `encapsulation dot1q vlan-id` | Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance. |
| 6    | `rewrite ingress tag {push (dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1q vlan-id dot1q vlan-id) | pop (1 | 2) | translate (1-to-1 (dot1q vlan-id | dot1ad vlan-id)| 2-to-1 dot1q vlan-id | dot1ad vlan-id) | 1-to-2 (dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id | dot1ad vlan-id dot1q vlan-id) | 2-to-2 (dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q | dot1ad vlan-id dot1q vlan-id) symmetric}` | Specifies the tag manipulation that is to be performed on the frame ingress to the service instance. |

### Examples

#### Single Tag VLAN Connect

This example shows an incoming frame with a dot1q tag of 10 enters TenGigabitEthernet 1/1. It is index directed to TenGigabitEthernet 1/2 and exits with a dot1q tag of 11. No MAC learning is involved.

Because there is a VLAN translation end to end, Layer2 protocol need to be carefully considered. Typically, the use case has both sides on the same encapsulation.

This example shows a typical configuration of a DSLAM facing port of the first PE router.

```
! DSLAM facing port
Router# enable
Router# configure terminal
```
Flexible QinQ Mapping and Service Awareness

Chapter 4  Configuring Layer 1 and Layer 2 Features

Router(config)# interface TenGigabitEthernet 1/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
!L2 facing port
Router(config)# interface TenGigabitEthernet 1/2
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 11
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
! connect service
Router(config)# connect EVC1 TenGigabitEthernet 1/1 100 TenGigabitEthernet 1/2 101

Double Tag VLAN Connect

In this example, an incoming frame with an outer dot1q tag of 10 and inner tag of 20 enters TenGigabitEthernet 1/1. It is index directed to TenGigabitEthernet 1/2 and exits with an outer dot1q tag of 11 and inner tag 21. No MAC learning is involved.

This example shows a typical configuration of a MPLS core facing port of the first PE router.

! DSLAM facing port
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 1/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 10 second-dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
!L2 facing port
Router(config)# interface TenGigabitEthernet 1/2
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 11 second-dot1q 21
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
! connect service
Router(config)# connect EVC1 TenGigabitEthernet 1/1 100 TenGigabitEthernet 1/2 101

Selective QinQ with Xconnect

This configuration uses EoMPLS under the single tag subinterface to forward packets. This example shows a typical configuration of a MPLS core facing port of the second PE router.

DSLAM facing port
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 1/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 10-20,30,50-60
Router(config-if-srv)# xconnect 2.2.2.2 999 pw-class vlan-xconnect
!
Router(config)# interface Loopback1
Router(config-if)# ip address 1.1.1.1 255.255.255.255

MPLS core facing port
Router(config)# interface TenGigabitEthernet 2/1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# mpls ip
Flexible QinQ Mapping and Service Awareness

Router(config-if)# mpls label protocol ldp

MPLS core facing port

Router(config)# interface TenGigabitEthernet 2/1
Router(config-if)# ip address 192.168.1.2 255.255.255.0
Router(config-if)# mpls ip
Router(config-if)# mpls label protocol ldp

CE facing EoMPLS configuration

Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 1/2
Router(config-if)# service instance 1000
Router(config-if-srv)# encapsulation dot1q 1000 second-dot1q any
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# xconnect 1.1.1.1 999 pw-class vlan-xconnect

Selective QinQ with Layer 2 Switching

This configuration uses Layer 2 Switching to perform packet forwarding. The forwarding mechanism is the same as MPBE; only the rewrites for each service instance are different.

DSLAM facing port, single tag incoming

Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 1/1
Router(config-if)# service instance 1000 ethernet
Router(config-if-srv)# encapsulation dot1q 10-20
Router(config-if-srv)# bridge-domain 11

QinQ VLAN

Router(config)# interface TenGigabitEthernet 1/2
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk vlan allow 11

Double Tag Translation (2-to-2 Tag Translation)

In this configuration, double-tagged frames are received on ingress. Both tags are popped and two new tags are pushed. The packet is then Layer 2 switched to the bridge domain VLAN.

QinQ facing port

Router(config)# interface TenGigabitEthernet 1/1
Router(config-if)# service instance 1000 ethernet
Router(config-if-srv)# encapsulation dot1q 100 second-dot1q 10
Router(config-if-srv)# rewrite ingress tag translate 2-to-2 dot1q 200 second-dot1q 20 symmetric
Router(config-if-srv)# bridge-domain 200

QinQ VLAN

Router(config)# interface TenGigabitEthernet 1/2
Double Tag Termination (2 to 1 Tag Translation)

The configuration in this example uses the Layer 2 switching.

Double tag traffic

Router(config)# interface TenGigabitEthernet 1/1
Router(config)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 200 second-dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-if-srv)# bridge-domain 10
!
Router(config)# interface TenGigabitEthernet 1/2
Router(config)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 200 second-dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-if-srv)# bridge-domain 10
!
Router(config)# interface TenGigabitEthernet 1/3
Router(config)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 30
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 10

Verification

Use these commands to verify operation.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ethernet service evc [id evc-id</td>
<td>interface interface-id] [detail]</td>
</tr>
<tr>
<td>Router# show ethernet service instance [id instance-id</td>
<td>interface interface-id] [interface interface-id] [detail]</td>
</tr>
<tr>
<td>Router# show ethernet service interface [interface-id] [detail]</td>
<td>Displays information in the Port Data Block (PDB).</td>
</tr>
<tr>
<td>Router# show mpls l2 transport vc detail</td>
<td>Displays details of the virtual connection (VC).</td>
</tr>
<tr>
<td>Router# show mpls forwarding</td>
<td>Displays the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB). Note: Output should have the label entry l2ckt.</td>
</tr>
</tbody>
</table>

Note
Troubleshooting

Use these debug commands to troubleshoot Flexible QinQ feature.

Debug commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show connect</td>
<td>Displays statistics and other information about Frame-Relay-to-ATM Network Interworking (FRF.5) and Frame Relay-to-ATM Service Interworking (FRF.8) connections.</td>
</tr>
<tr>
<td>Router# show xconnect</td>
<td>Displays information about cross-connect attachment circuits and pseudowires.</td>
</tr>
</tbody>
</table>

Table 4-4 provides the troubleshooting solutions for the Flexible mapping feature.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erroneous TCAM entries.</td>
<td>Use the <code>show hw-module subslot subslot tcam</code> command to verify and the TCAM entries. Share the output with TAC for further investigation.</td>
</tr>
<tr>
<td>Incorrect virtual VLAN IDs on a QinQ subinterface.</td>
<td>Use the <code>test hw-mod subslot subslot</code> command to verify the virtual VLAN ID values on a QinQ subinterface. Share the output with TAC for further investigation.</td>
</tr>
</tbody>
</table>
Configuring MultiPoint Bridging over Ethernet on Cisco 7600 Series ES+ Line Cards

MultiPoint Bridging over Ethernet (MPBE) on Cisco 7600 Series ES+ line cards provides Ethernet LAN switching with MAC learning, local VLAN significance, and full QoS support. MPBE also provides Layer 2 switchport-like features without the full switchport implementation. MPBE is supported only through Ethernet Virtual Connection Services (EVCS) service instances.

EVCS uses the concepts of EVCs (Ethernet virtual circuits) and service instances. An EVC is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider to a customer. It embodies the different parameters on which the service is being offered. A service instance is the instantiation of an EVC on a given port on a given router.

For MPBE, an EVC packet filtering capability prevents leaking of broadcast/multicast bridge-domain traffic packets from one service instance to another. Filtering occurs before and after the rewrite to ensure that the packet goes only to the intended service instance.

You can use MPBE to:

- Simultaneously configure Layer 2 and Layer 3 services such as Layer 2 VPN, Layer 3 VPN, and Layer 2 bridging on the same physical port.
- Define a broadcast domain in a system. Customer instances that are part of a broadcast domain can be in the same physical port or in different ports.
- Configure multiple service instances with different encapsulations and map them to a single bridge domain.
- Perform local switching between service instances under the same bridge domain.
- Perform local switching across different physical interfaces using service instances that are part of the same bridge domain.
- Replicate flooded packets from the core to all service instances under the bridge domain.
- Configure a Layer 2 tunneling service or Layer 3 terminating service under the bridge domain VLAN.

MPBE accomplishes this by manipulating VLAN tags for each service instance and mapping the manipulated VLAN tags to Layer 2 or Layer 3 services. Possible VLAN tag manipulations include:

- Single tag termination

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong interface configured and tag manipulation incorrectly programmed.</td>
<td>Use the command <code>show platform np interface detail</code> to verify the interface and tag details. Share the output with TAC for further investigation.</td>
</tr>
<tr>
<td>VLAN ID is incorrectly programmed</td>
<td>Use the command <code>show hw-module subslot subslot tcam all_entries vlan</code> to verify the VLAN ID details. Share the output with TAC for further investigation.</td>
</tr>
<tr>
<td>Inner, outer start/end VLANs incorrectly programmed.</td>
<td>Use the <code>show platform np efp</code> command to verify the VLAN details. Share the output with TAC for further investigation.</td>
</tr>
<tr>
<td>Erroneous TCAM entries on the platform</td>
<td>Use the <code>show platform np efp</code> and <code>show platform np efp all_entries vlan</code> commands to verify the VLAN details. Share the output with TAC for further investigation.</td>
</tr>
</tbody>
</table>
• Single tag tunneling
• Single tag translation
• Double tag termination
• Double tag tunneling
• Double tag translation
• Selective QinQ translation

Restrictions and Usage Guidelines

When configuring the MPBE over Ethernet on Cisco 7600 Series ES+ line cards, follow these restrictions and usage guidelines:
• Each service instance is considered as a separate circuit under the bridge-domain.
• Encapsulation can be dot1q or QinQ packets.
• 440 MPB VCs are supported under one bridge-domain (110 per network processor).
• IGMP snooping is supported with MPB VCs as long as the service instance is terminated on the bridge-domain (must pop all tags, symmetric).
• Split Horizon is supported with MPB VCs.
• Untagged BPDU packets can be peered, dropped, or forwarded as data.
• Tagged BPDU packets can be dropped or forwarded as data.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface gigabitethernet slot/port` or `interface tengigabitethernet slot/port`
4. `[no] service instance id {Ethernet [service-name]}`
5. `encapsulation dot1q vlan-id [second-dot1q vlan-id]`
6. `[no] rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} } symmetric`
7. `[no] bridge-domain bridge-id`
## DETAILED STEPS

<table>
<thead>
<tr>
<th></th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>interface gigabitethernet slot/port or interface tengigabitethernet slot/port</td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where:</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• slot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td>4</td>
<td>[no] service instance id {Ethernet [service-name]}</td>
<td>Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td>5</td>
<td>encapsulation dot1q vlan-id [second-dot1q vlan-id]</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td>6</td>
<td>[no] rewrite ingress tag {push {dot1q vlan-id</td>
<td>dot1q vlan-id second-dot1q vlan-id</td>
</tr>
<tr>
<td></td>
<td>| pop {1</td>
<td>2}</td>
</tr>
<tr>
<td>7</td>
<td>[no] bridge-domain bridge-id</td>
<td>Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.</td>
</tr>
</tbody>
</table>
Examples

Single Tag Termination Example

In this example, the single tag termination identifies customers based on a single VLAN tag and maps the single-VLAN tag to the bridge-domain.

Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 1/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 12

Single Tag Tunneling Example

In this single tag tunneling example, the incoming VLAN tag is not removed but continues with the packet.

Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 1/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# bridge-domain 200

Single Tag Translation Example

In this single-tag translation example, the incoming VLAN tag is removed and VLAN 200 is added to the packet.

Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 3/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag translate 1-to-1 dot1q 200 symmetric
Router(config-if-srv)# bridge-domain 200

Double Tag Tunneling Example

In this double tag tunneling example, the incoming VLAN tags are not removed but continue with the packet.

Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 1/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10 second-dot1q 20
Router(config-if-srv)# bridge-domain 200

Double Tag Termination Configuration Example

In this double-tag termination example, the ingress receives double tags that identify the bridge VLAN; the double tags are stripped (terminated) from the packet.
Double-Tag Translation Configuration Example

In this example, double tagged frames are received on ingress. Both tags are popped and two new tags are pushed. The packet is then Layer-2-switched to the bridge-domain VLAN.

```
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 2/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10 inner 20
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-if-srv)# bridge-domain 200
```

```
Router(config-if-srv)# service instance 2
Router(config-if-srv)# encapsulation dot1q 40 inner 30
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-if-srv)# bridge-domain 200
```

Selective QinQ Configuration Example

In this example, a range of VLANs is configured and plugged into a single MPB VC.

```
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10-20
Router(config-if-srv)# bridge-domain 200
```

```
Router(config-if-srv)# encapsulation dot1q 10-20
Router(config-if-srv)# bridge-domain 200
```

Untagged Traffic Configuration Example

In this example, untagged traffic is bridged to the bridge domain and forwarded to the switchport trunk.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# no ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation untagged
Router(config-if-srv)# bridge-domain 11
```

```
Router(config-if-srv)# interface TenGigabitEthernet 1/1
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
```
Router(config-if)# switchport trunk allowed vlan 11

**MPBE with Split Horizon Configuration Example**

In this example, unknown unicast traffic is flooded on the bridge domain except for the interface from which the traffic originated.

```plaintext
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# no ip address
Router(config-if)# service instance 1000 ethernet
Router(config-if-srv)# encapsulation dot1q 100 second-dot1q 10-20
Router(config-if-srv)# bridge-domain 100 split-horizon
Router(config-if)# service instance 1001 ethernet
Router(config-if-srv)# encapsulation dot1q 101 second-dot1q 21-30
Router(config-if-srv)# bridge-domain 101 split-horizon
Router(config-if)# service instance 1010 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# rewrite ingress tag symmetric translate 1-to-2 dot1q 10 second-dot1q 100 symmetric
Router(config-if-srv)# bridge-domain 10 split-horizon
Router(config-if)# mls qos trust dscp
```

In this example, service instances are configured on Ethernet interfaces and terminated on the bridge domain.

```plaintext
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 1000
Router(config-if-srv)# bridge-domain 10

Router(config)# interface GigabitEthernet 1/1
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk allowed vlan 10
```

**Verification**

Use these commands to verify operation.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ethernet service evc [id evc-id</td>
<td>interface interface-id] [detail]</td>
</tr>
<tr>
<td>Router# show ethernet service instance [id instance-id</td>
<td>interface interface-id</td>
</tr>
</tbody>
</table>
Chapter 4  Configuring Layer 1 and Layer 2 Features

Backup Interface for Flexible UNI

The Backup Interface for Flexible UNI feature allows you to configure redundant user-to-network interface (UNI) connections for Ethernet interfaces, which provides redundancy for dual-homed devices.

You can configure redundant (flexible) UNIs on a network provider-edge (N-PE) device in order to supply flexible services through redundant user provider-edge (U-PE) devices. The UNIs on the N-PEs are designated as primary and backup and have identical configurations. If the primary interface fails, the service is automatically transferred to the backup interface.

Figure 4-2 shows an example of how Flexible UNIs can be used when the Cisco 7600 series router is configured as a dual-homed N-PE (NPE1) and as a dual-homed U-PE (UPE2).

Figure 4-2  Backup Interface for Dual-Homed Devices

Note  The configurations on the primary and backup interfaces must be identical.

The primary interface is the interface for which you configure a backup. During operation, the primary interface is active and the backup (secondary) interface operates in standby mode. If the primary interface goes down (due to loss of signal), the router begins using the backup interface.

While the primary interface is active (up) the backup interface is in standby mode. If the primary interface goes down, the backup interface transitions to the up state and the router begins using it in place of the primary. When the primary interface comes back up, the backup interface transitions back to standby mode. While in standby mode, the backup interface is effectively down and the router does not monitor its state or gather statistics for it.

This feature provides the following benefits:

- Supports the following Ethernet virtual circuit (EVC) features:
  - Frame matching: EVC with any supported encapsulation (Dot1q, default, untagged).
  - Frame rewrite: Any supported (ingress and egress with push, pop, and translate).

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ethernet service interface [interface-id] [detail]</td>
<td>Displays information in the Port Data Block (PDB).</td>
</tr>
<tr>
<td>Router# show ethernet service instance summary</td>
<td>Displays the overall count for service instance as well as the service instance count for individual interfaces.</td>
</tr>
</tbody>
</table>
– Frame forwarding: MultiPoint Bridging over Ethernet (MPBE), xconnect, connect.
– Quality of Service (QoS) on EVC.
• Supports Layer 3 (L3) termination.
• Supports several types of uplinks: MultiProtocol Label Switching (MPLS), Virtual Private LAN Service (VPLS), and switchports.

The Backup Interface for Flexible UNI feature makes use of these Ethernet components:
• Ethernet virtual circuit (EVC)—An association between two or more UNIs that identifies a point-to-point or point-to-multipoint path within the provider network. For more information about EVCs, see the “Troubleshooting” section on page 4-20.
• Ethernet flow point (EFP)—The logical demarcation point of an EVC on an interface. An EVC that uses two or more UNIs requires an EFP on the associated ingress interface and egress interface of every device that the EVC passes through.

Restriction and Usage Guidelines

Observe these restrictions and usage guidelines as you configure a backup interface for Flexible UNI on the router:
• Hardware and software support:
  – Supported on Cisco 7600 Series ES+ and ES20 line cards.
  – Supported with the Route Switch Processor 720 and Supervisor Engine 720.
  – Requires Cisco IOS Release 12.2(33)SRD or later.
• You can use the same IP address on both the primary and secondary interfaces. This enables the interface to support L3 termination (single or double tagged).
• The configurations on the primary and backup interfaces must match. The router does not check that the configurations match; however, the feature does not work if the configurations are not the same.
  
  **Note** If the configuration includes the `xconnect` command, you must specify a different VCID on the primary and backup interfaces.

• The duplicate resources needed for the primary and secondary interfaces are taken from the total resources available on the router and thus affect available resources. For example, each `xconnect` command consumes resources on both the primary and backup interfaces.
• Any features configured on the primary and backup interfaces (such as `bridge-domain`, `xconnect`, and `connect` commands) transition up or down as the interface itself transitions between states.
• Switchover time between primary and backup interfaces is best effort. The time it takes the backup interface to transition from standby to active mode depends on the link-state detection time and the amount of time needed for EVCs and their features to transition to the up state.
• Configuration changes and administrative actions made on the primary interface are automatically reflected on the backup interface.
• The router monitors and gathers statistics for the active interface only, not the backup. During normal operation, the primary interface is active; however, if the primary goes down, the backup becomes active and the router begins monitoring and gathering statistics for it.
When the primary interface comes back up, the backup interface always transitions back to standby mode. Once the signal is restored on the primary interface, there is no way to prevent the interface from being restored as the primary.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `backup interface type interface`

**Note** You must apply the same configuration to both the primary and backup interfaces or the feature does not work. To configure EVC service instances on the interfaces, use the `service instance`, `encapsulation`, `rewrite`, `bridge-domain`, and `xconnect` commands. For information, see the “Configuring MultiPoint Bridging over Ethernet on Cisco 7600 Series ES+ Line Cards” section on page 4-32 and the “Configuring Any Transport over MPLS” section on page 6-1.

5. (Optional) `backup delay enable-delay disable-delay`
6. (Optional) `backup load enable-percent disable-percent`
7. `exit`
8. (Optional) `connect primary interface srv-inst interface srv-inst`
9. (Optional) `connect backup interface srv-inst interface srv-inst`
10. (Optional) `connect primary interface srv-inst1 interface srv-inst2`
11. (Optional) `connect backup interface srv-inst1 interface srv-inst2`
12. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| Example: | Router# enable | |
| Step 2 | `configure terminal` | Enters global configuration mode. |
| Example: | Router# configure terminal | |
| Step 3 | `Router(config)# interface type slot/port` | Selects the primary interface. This is the interface you are creating a backup interface for. For example, `interface gigabitEthernet 3/1` selects the interface for port1 of the Gigabit Ethernet card installed in slot 3.  
- `type` specifies the interface type. Valid values are `gigabitethernet` or `tengigabitethernet`.  
- `slot/port` specifies the location of the interface. |
| Example: | Router(config)# interface gigabitethernet 3/1 | |
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Router(config-if)# <strong>backup interface</strong> type interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)# backup interface gigabitethernet 4/1</td>
</tr>
</tbody>
</table>

**Purpose**

Selects the interface to serve as a backup interface.

**Note**
You must apply the same configuration to both the primary and backup interfaces or the feature does not work.

To configure EVC service instances on the interfaces, use the **service instance**, **encapsulation**, **rewrite**, **bridge-domain**, and **xconnect** commands. For information, see the “Configuring MultiPoint Bridging over Ethernet on Cisco 7600 Series ES+ Line Cards” section on page 4-32 and the “Configuring Any Transport over MPLS” section on page 6-1.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Router(config-if)# <strong>backup delay</strong> enable-delay disable-delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-if)# backup delay 0 0</td>
</tr>
</tbody>
</table>

(Optional) Specifies a time delay (in seconds) for enabling or disabling the backup interface.

- **enable-delay** is the amount of time to wait after the primary interface goes down before bringing up the backup interface.
- **disable-delay** is the amount of time to wait after the primary interface comes back up before restoring the backup interface to the standby (down) state

**Note**
For the backup interface for Flexible UNI feature, do not change the default delay period (0 0) or the feature may not work correctly.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Router(config-if)# <strong>backup load</strong> enable-percent disable-percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-if)# backup load 50 10</td>
</tr>
</tbody>
</table>

(Optional) Specifies the thresholds of traffic load on the primary interface (as a percentage of the total capacity) at which to enable and disable the backup interface.

- **enable-percent**—Activate the backup interface when the traffic load on the primary exceeds this percentage of its total capacity.
- **disable-percent**—Deactivate the backup interface when the combined load of both primary and backup returns to this percentage of the primary interface’s capacity.

Applying the settings from the example to a primary interface with 10-Mbyte capacity, the router enables the backup interface when traffic load on the primary exceeds 5 mb (50%), and disables the backup when combined traffic on both interfaces falls below 1 Mbyte (10%).

<table>
<thead>
<tr>
<th>Step 7</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-if)# exit</td>
</tr>
</tbody>
</table>

Exits interface configuration mode and returns to global configuration mode.
### Backup Interface for Flexible UNI

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> Router(config)# <strong>connect primary</strong> interface srv-inst interface srv-inst</td>
<td>(Optional) Creates a local connection between a single service instance (srv-inst) on two different interfaces. The <strong>connect primary</strong> command creates a connection between primary interfaces.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# connect primary gi3/2 gi3/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> Router(config)# <strong>connect backup</strong> interface srv-inst interface srv-inst</td>
<td>(Optional) Creates a local connection between a single service instance (srv-inst) on two different interfaces. The <strong>connect backup</strong> command creates a connection between backup interfaces.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# connect backup gi4/2 gi4/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> Router(config)# <strong>connect primary</strong> interface srv-inst1 interface srv-inst2</td>
<td>(Optional) Enables local switching between different service instances (srv-inst1 and srv-inst2) on the same port. Use the <strong>connect primary</strong> command to create a connection on a primary interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# connect primary gi3/2 gi3/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> Router(config)# <strong>connect backup</strong> interface srv-inst1 interface srv-inst2</td>
<td>(Optional) Enables local switching between different service instances (srv-inst1 and srv-inst2) on the same port. Use the <strong>connect backup</strong> command to create a connection on a backup interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# connect backup gi4/2 gi4/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Note** If you have configured any interface (L3, Switchport, or EVC) using the **backup interface** command, then you are not supposed to run the **shutdown** command on the active interface. If you run **shutdown**, then the standby interface will also go down.

The following example shows a sample configuration in which:

- gi3/1 is the primary interface and gi4/1 is the backup interface.
- Each interface supports two service instances (2 and 4), and each service instance uses a different type of forwarding (**bridge-domain** and **xconnect**).
- The **xconnect** command for service instance 2 uses a different VCID on each interface.

```bash
Router# enable
Router# configure terminal
Router(config)# interface gi3/1
Router(config-if)# backup interface gi4/1
Router(config-if)# service instance 4 ethernet
Router(config-if-srv)# encapsulation dot1q 4
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 4
Router(config-if-srv)# exit
Router(config-if)# service instance 2 ethernet
Router(config-if-srv)# encapsulation dot1q 2
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
```
Backup Interface for Flexible UNI

Chapter 4  Configuring Layer 1 and Layer 2 Features

Router(config-if-srv)# xconnect 10.0.0.0 2 encaps mpls

Router(config)# interface gi4/1

Router(config-if)# service instance 4 ethernet
Router(config-if-srv)# encapsulation dot1q 4
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 4
Router(config-if-srv)# exit

Router(config-if)# service instance 2 ethernet
Router(config-if-srv)# encapsulation dot1q 2
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric

Verification

This section lists the commands to display information about the primary and backup interfaces configured on the router. In the examples that follow, the primary interface is gi3/1 and the secondary (backup) interface is gi3/11.

- To display a list of backup interfaces, use the show backup command in privileged EXEC mode. Our sample output shows a single backup (secondary) interface:

```
Router# show backup
Primary Interface   Secondary Interface   Status
-----------------   -------------------   ------
GigabitEthernet 3/1 GigabitEthernet 3/11 normal operation
```

- To display information about a primary or backup interface, use the show interfaces command in privileged EXEC mode. Issue the command on the interface for which you want to display information. The following examples show the output displayed when the command is issued on the primary (gi3/1) and backup (gi3/11) interfaces:

```
Router# show interface gi3/1
GigabitEthernet3/1 is up, line protocol is up (connected)
Hardware is GigEther SPA, address is 0005.dc57.8800 (bia 0005.dc57.8800)
Backup interface GigabitEthernet 3/11, failure delay 0 sec, secondary disable delay 0 sec, kickin load not set, kickout load not set [...]

Router# show interface gi3/11
GigabitEthernet3/11 is standby mode, line protocol is down (disabled)
```

If the primary interface goes down, the backup (secondary) interface is transitioned to the up state, as shown in the command output that follows. Notice how the command output changes if you reissue the show backup and show interfaces commands at this time: the show backup status changes, the line protocol for gi3/1 is now down (notconnect), and the line protocol for gi3/11 is now up (connected).

```
Router# !!! Link gi3/1 (active) goes down...
22:11:11: %LINK-DFC3-3-UPDOWN: Interface GigabitEthernet3/1, changed state to down
22:11:12: %LINK-DFC3-3-UPDOWN: Interface GigabitEthernet3/11, changed state to up
22:11:12: %LINEPROTO-DFC3-5-UPDOWN: Line protocol on Interface GigabitEthernet3/1, changed state to down

Router# show backup
Primary Interface   Secondary Interface   Status
-----------------   -------------------   ------
```
Chapter 4 Configuring Layer 1 and Layer 2 Features

Backup Interface for Flexible UNI

---

GigabitEthernet3/1 GigabitEthernet3/11 backup mode

Router# show interface gi3/1
GigabitEthernet3/1 is down, line protocol is down (notconnect)
  Hardware is GigEther SPA, address is 0005.dc57.8800 (bia 0005.dc57.8800)
  Backup interface GigabitEthernet3/11, failure delay 0 sec, secondary disable delay 0 sec.

Router# show interface gi3/11
GigabitEthernet3/11 is up, line protocol is up (connected)

Verification: show interface Command

If slot 2 on the router has an ES+ 40 LC (primary interface), and slot 3 has ES 20 LC (backup interface), the show interface command displays the following output:

```
7609-PE-AGG-1#show backup
Primary Interface          Secondary Interface        Status
-------------------------  -------------------------  -----
GigabitEthernet2/24        GigabitEthernet3/0/6       normal operation
7609-PE-AGG-1#sh int gi2/24
GigabitEthernet2/24 is up, line protocol is up (connected)
  Hardware is X40G 1Gb 802.3, address is 6400.f175.9e00 (bia 6400.f175.9e00)
  Description: *******Connected to UPE-1 Gig2/24********
  Backup interface GigabitEthernet3/0/6, failure delay 0 sec, secondary disable delay 0 sec,
  kickin load not set, kickout load not set
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, clock source internal, media type is SX
  input flow-control is off, output flow-control is off
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:42, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: Class-based queueing
  Output queue: 0/40 (size/max)
  5 minute input rate 7441000 bits/sec, 1117 packets/sec
  5 minute output rate 3550000 bits/sec, 641 packets/sec
  L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
  L3 in Switched: ucast: 745 pkt, 362690 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
  9464396 packets input, 777474638 bytes, 0 no buffer
  Received 4101619 broadcasts (0 IP multicasts)
  0 runs, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  0 input packets with dribble condition detected
  5457466 packets output, 3714363660 bytes, 0 underruns
  0 output errors, 0 collisions, 2 interface resets
  0 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out
7609-PE-AGG-1#sh int gi3/0/6
GigabitEthernet3/0/6 is standby mode, line protocol is down (disabled)
  Hardware is GigEther SPA, address is 6400.f175.9e00 (bia 6400.f175.9e00)
  Description: **connected to UPE-1 Gig2/6 **
```
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, 
   reliability 255/255, txload 0/255, rxload 0/255 
Encapsulation ARPA, loopback not set 
Keepalive not supported 
Full-duplex, 1000Mb/s 
input flow-control is off, output flow-control is off 
Clock mode is auto 
ARP type: ARPA, ARP Timeout 04:00:00 
Last input never, output never, output hang never 
Last clearing of 'show interface' counters never 
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0 
Queueing strategy: fifo 
Output queue: 0/40 (size/max) 
5 minute input rate 0 bits/sec, 0 packets/sec 
5 minute output rate 0 bits/sec, 0 packets/sec 
L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes 
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast 
L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes 
   0 packets input, 0 bytes, 0 no buffer 
Received 0 broadcasts (0 IP multicasts) 
0 runts, 0 giants, 0 throttles 
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 
0 watchdog, 0 multicast, 0 pause input 
0 input packets with dribble condition detected 
0 packets output, 0 bytes, 0 underruns 
0 output errors, 0 collisions, 0 interface resets 
0 unknown protocol drops 
0 babbles, 0 late collision, 0 deferred 
0 lost carrier, 0 no carrier, 0 pause output 
0 output buffer failures, 0 output buffers swapped out 

Note

On ES+ line cards, when you run the show interface command, Layer 2 multicast packets are accounted under the Broadcast category.

Example

Figure 4-3 shows a sample configuration of a backup interface for Flexible UNI. The configuration includes several EVCs (service instances), configured as follows:

- Service instance 4 is configured on primary and backup interfaces (links) that terminate in a bridge domain, with a VPLS uplink onto network provider edge NPE12.
- Service instance 2 is configured as scalable Ethernet over MPLS, peering with an SVI VPLS on NPE12.
Figure 4-3  Backup Interface for Flexible UNI Configuration

This is the configuration at NPE10:

```plaintext
interface ge2/4.4
  description npe10 to npe11 gi3/11 – backup – bridged
  encapsulation dot1q 4
  ip address 100.4.1.33 255.255.255.0

interface ge2/4.2
  description npe10 to npe11 gi3/11 – backup – xconnect
  encapsulation dot1q 2
  ip address 100.2.1.33 255.255.255.0
```

This is the configuration at NPE14:

```plaintext
interface ge1/3.4
  description npe14 to npe11 gi3/1 – primary – bridged
  encapsulation dot1q 4
  ip address 100.4.1.22 255.255.255.0

interface ge1/3.2
  description npe14 to npe11 gi3/1 – primary – xconnect
  encapsulation dot1q 2
  ip address 100.2.1.22 255.255.255.0
```

This is the configuration at 72a, at the user-facing provider edge (U-PE):

```plaintext
interface fa1/0.4
  description 72a to npe12 – bridged
  encapsulation dot1q 4
  ip address 100.4.1.12 255.255.255.0

interface fa1/0.2
  description 72a to npe12 – xconnect
  encapsulation dot1q 2
  ip address 100.2.1.12 255.255.255.0
```

This is the configuration at NPE11:

```plaintext
interface gigabitEthernet 3/1
  backup interface gigabitEthernet 3/11
  service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  xconnect 12.0.0.1 2 encapsulation mpls
  service instance 4 ethernet
  encapsulation dot1q 4
  rewrite ingress tag pop 1 symmetric
  bridge-domain 4
```
interface gigabitEthernet 3/11
  service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  xconnect 12.0.0.1 21 encapsulation mpls
service instance 4 ethernet
  encapsulation dot1q 4
  rewrite ingress tag pop 1 symmetric
  bridge-domain 4

This is the configuration at NPE12:

interface GE-WAN 4/3
  description npe11 to npe12
  ip address 10.3.3.1 255.255.255.0
  mpls ip
12 vfi vlan4 manual
  vpn id 4
  neighbor 12.0.0.1 4 encapsulation mpls
interface Vlan 4
  xconnect vfi vlan4
12 vfi vlan4 manual
  vpn id 4
  neighbor 11.0.0.1 4 encap mpls
interface Vlan4
  description npe12 to npe11 xconnect
  xconnect vfi vlan4
12 vfi vlan2 manual
  vpn id 2
  neighbor 11.0.0.1 2 encap mpls
  neighbor 11.0.0.1 21 encap mpls
interface Vlan2
  xconnect vfi vlan2
interface GE-WAN 9/4
  description npe12 to npe11
  ip address 10.3.3.2 255.255.255.0
  mpls ip

interface fastEthernet 8/2
  description npe12 to 72a
  switchport
  switchport trunk encap dot1q
  switchport mode trunk
  switchport trunk allowed vlan 2-4

The primary interface is enabled:

NPE 11# show backup
  Primary interface Secondary interface Status
  ---------------------------------------------
  GigabitEthernet3/1 GigabitEthernet3/11 normal operation
NPE-11#sh int gi3/1
  GigabitEthernet3/1 is up, line protocol is up (connected)
  Hardware is GigEther SPA, address is 0005.dc57.8800(bia 0005.dc57.8800)
  Backup interface GigabitEthernet3/11, failure delay 0 sec, secondary disable delay 0 sec,kicking load not set, kickout load not set,
  [...]  
NPE-11# show interface gi3/11
  GigabitEthernet 3/11 is standby mode, line protocol is down (disabled)

The primary link is disabled:

NPE 11#!!!Link gi3/1 (active) goes down
Troubleshooting

Table 4-5 provides troubleshooting solutions for the backup interface of the Flexible UNI feature.

Table 4-5  Troubleshooting Scenarios for backup interface of the Flexible UNI feature

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The backup interface is in a standby state or the line protocol is down</td>
<td>Use the <code>show interfaces</code> command on the specific interface in privileged EXEC mode to display interface and line protocol details. Share the output with TAC for further investigation. This sample output of the command is displayed when the command on the primary (gi3/0/0) and backup (gi3/0/11) interfaces:</td>
</tr>
<tr>
<td></td>
<td>NPE-11# show int gi3/0/0</td>
</tr>
<tr>
<td></td>
<td>GigabitEthernet3/0/0 is up, line protocol is up (connected)</td>
</tr>
<tr>
<td></td>
<td>Hardware is GigEther SPA, address is 0005.dc57.8800 (bia 0005.dc57.8800)</td>
</tr>
<tr>
<td></td>
<td>Backup interface GigabitEthernet3/0/11, failure delay 0 sec, secondary disable delay 0 sec</td>
</tr>
<tr>
<td></td>
<td>NPE-11# show int gi3/11</td>
</tr>
<tr>
<td></td>
<td>GigabitEthernet3/11 is up, line protocol is up (connected)</td>
</tr>
</tbody>
</table>

EVC on Port-Channel

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links. The EVC EtherChannel feature provides support for EtherChannels on Ethernet Virtual Connection Services (EVCS) service instances.
For more information on EtherChannels, and how to configure EtherChannels on Layer 2 or Layer 3 LAN ports, see Configuring EtherChannels at http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/channel.html.

The EVC EtherChannel feature supports MPBE, local connect, and xconnect service types. Load balancing is accomplished on a Ethernet flow point (EFP) basis where a number of EFPs exclusively pass traffic through member links. In a default load balancing, you have no control over how the EFPs are grouped together, and sometimes the EFP grouping may not be ideal. To avoid this, use manual load balancing to control the EFP grouping.

Restrictions and Usage Guidelines

When configuring EVC EtherChannel, follow these restrictions and usage guidelines:

- All member links of the port-channel are on Cisco 7600-ES+ line cards.
- Bridge-domain, xconnect, connect EVCs, switchports, and IP subinterfaces are allowed over the port-channel interface and the main interface.
- The EFP limit decreases with the number of member links on the NP. For instance, if there are 4 members within the same NP, the EVC limit on the NP decreases to 2000, that is (8000/4).

**Note** For a switchport (not for data traffic), use the `service instance ethernet` command to create a service instance to support OAM requirements.

- If you configure a physical port as part of a channel group, you cannot configure EVCs under that physical port.
- A physical port that is part of an EVC port-channel cannot have switchport configuration.
- Total number of port channels EVCs per box is 16000.
- Statically configuring port-channel membership with LACP is not supported.
- You can apply QoS policies under EVCs on a port-channel with the exception that ingress microflow policing is not supported. For more information on configuring QoS with EVCs, see Configuring QoS, page 7-1.
- You cannot use the `bandwidth percent` or `police percent` commands on EVC port-channels in flat policy-maps or in parent of HQoS policy-maps.
- When EVC+xconnect is configured under the port-channel, the local VC label is also used to distribute the traffic load on the member links. In this case, when the port-channel flaps, the Xconnect also flaps. This will lead to a change in the load-distribution as the local VC label will also change. In those deployment scenarios where it is desired not to change the load-distribution when the port-channel flaps, two alternatives are recommended:
  - Configure the xconnect under an interface VLAN (SVI).
  - Use the manual load-balancing configuration to map xconnect to specific member links.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface port-channel number
4. `[no] ip address`  
5. `[no] service instance id Ethernet [service-name]`  
6. `encapsulation {default|untagged|dot1q vlan-id | second-dot1q vlan-id}`  
7. `rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id | second-dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id | second-dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 | 2-to-1 | 1-to-2 | 2-to-2 | symmetric}`  
8. `[no] bridge-domain bridge-id or xconnect vfi vfi name`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
`enable`  | Enables privileged EXEC mode.  
- Enter your password if prompted.  
**Example:**  
Router# enable |
| **Step 2**  
`configure terminal`  | Enters global configuration mode.  
**Example:**  
Router# configure terminal |
| **Step 3**  
`interface port-channel number`  | Creates the port-channel interface.  
**Example:**  
Router(config)# interface port-channel 11 |
| **Step 4**  
`[no] ip address`  | Assigns a subnet mask to the ethernet channel.  
**Example:**  
Router(config-if)# no ip address |
| **Step 5**  
`[no] service instance id Ethernet [service-name]`  | Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode.  
**Example:**  
Router(config-if)# service instance 101 ethernet |
| **Step 6**  
`encapsulation {default|untagged|dot1q vlan-id | second-dot1q vlan-id}`  | Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.  
**Example:**  
Router(config-if-srv)# encapsulation dot1q 13 |
### EVC on Port-Channel

**Step 7**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`rewrite ingress tag (push (dot1q vlan-id</td>
<td>Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-if-srv)# rewrite ingress
tag push dot1q 20 symmetric
```

**Step 8**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`</td>
<td>no</td>
</tr>
<tr>
<td><code>or</code></td>
<td><code>xconnect vfi vfi name</code></td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-if-srv)# bridge-domain 12
```

### Examples

This example shows a single port-channel interface is created with three possible member links from slots 1 and 2:

```
Router# enable
Router# configure terminal
Router(config)# interface Port-channel5
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# channel-group 5 mode on
```

This example shows scalable EomplS and EVC connect sample configuration.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 3/0/0
Router(config-if)# service instance 10 ethernet
Router(config-srv)# encapsulation dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 1 sym
Router(config-if-srv)# exit
Router(config-if)# exit
Router(config)# interface GigabitEthernet 3/0/1
Router(config-if)# service instance 12 ethernet
Router(config-srv)# encapsulation dot1q 30
Router(config-if-srv)# rewrite ingress tag pop 1 sym
Router(config-if-srv)# exit
Router(config-if)# exit
Router(config)# connect TEST GigabitEthernet 3/0/0 10 GigabitEthernet 3/0/1 12
Router# sh connection all
```

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Segment 1</th>
<th>Segment 2</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>TEST</td>
<td>G13/0/0:10</td>
<td>G13/0/1:12</td>
<td>UP</td>
</tr>
</tbody>
</table>

This is a typical QoS configuration.
Router# enable
Router# configure terminal
Router(config)# interface port-channel10
Router(config-if)# no ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 11
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if)# service-policy input x
Router(config-if)# service-policy output y
Router(config-if-srv)# bridge-domain 1500

Use the following commands to verify the configuration.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ethernet service evc [id evc-id</td>
<td>interface interface-id] [detail]</td>
</tr>
<tr>
<td>Router# show ethernet service instance interface port-channel number [summary]</td>
<td>Displays the summary of all the configured EVCs within the interface.</td>
</tr>
<tr>
<td>Router# show ethernet service instance [id instance-id</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Router# show mpls l2 transport vc detail</td>
<td>Displays detailed information related to the virtual connection (VC).</td>
</tr>
<tr>
<td>Router# show mpls forwarding</td>
<td>Displays the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB).</td>
</tr>
<tr>
<td>Note</td>
<td>Output should have the label entry l2ckt.</td>
</tr>
<tr>
<td>Router# show etherchannel summary</td>
<td>Displays view all EtherChannel groups states and ports.</td>
</tr>
<tr>
<td>Router# show policy-map interface service instance</td>
<td>Displays the policy-map information for a given service instance.</td>
</tr>
</tbody>
</table>

**Troubleshooting**

Table 4-6 provides the troubleshooting solutions for the EVC on a Port-Channel.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port data block issues in port channel</td>
<td>Use the show ethernet service interface [interface-id] [detail] command to view information on the port data. Share the output with TAC for further investigation.</td>
</tr>
<tr>
<td>Issues with platform events or errors</td>
<td>Use the debug platform npc custom-ether client [event, error] command to debug and trace platform issues. Share the output with TAC for further investigation.</td>
</tr>
</tbody>
</table>
Configuring SPAN on EVC

Currently, traffic mirroring, lawful intercept, or Switched Port Analyzer (SPAN) on a per service instance is unavailable.

The existing command line interface supports configuring interface and VLAN as the local SPAN source. The same command line interface is enhanced to accept service instance IDs along with the interface. Since an EVC is support only for the local session SPAN, service instance options for the SPAN source are added in the local SPAN configuration submode.

You configure SPAN to intercept traffic in three ways:

- **SPAN on Port:** The traffic on all EVCs on the port or port channel is included for a SPAN session along with routed traffic on that port.
- **SPAN on VLAN:** The traffic on all EVC bridge-domains with the same VLAN is included for a SPAN session along with other switchports on the same VLAN.
- **SPAN on EVC:** The traffic on a given EFP or a set of EFPs is included for a SPAN session.

**Restrictions and Usage Guidelines**

Follow these restrictions and usage guidelines while configuring SPAN on EVC, follow these restrictions and usage guidelines:

- Only Local SPAN is supported.
- EVC SPAN is effective only if the EVC is on the ES+ line card.
- EVC as a SPAN destination is not supported.
- Egress SPAN packet does not undergo QoS processing.
- If a combination of switchports and EVC bridge-domain exists, then for flood case packet on both is spanned. VLAN and SPAN are configured in the transmit direction on the source port.
- If a combination of different EVC bridge-domain exists, then for flood case packet on all the EVCs is spanned. VLAN and SPAN are configured in the transmit direction on the source port.
- EVC SPAN does not work with multiple destination ports.
- For EVCs configured as a part of more than one SPAN session (EVC, VLAN, or port), traffic is monitored on only one session.
- EFPs and VLAN cannot be configured as source in the same monitor session.
- For a 10G port, the aggregate of ingress traffic and SPAN traffic cannot exceed 10G.
- For a 10G port with port-shaper, the aggregate of port traffic and SPAN traffic cannot exceed the port-shaper.
- For a 1G port, the total SPAN traffic can be as high as 10G, but due to network processor limitations and fabric bottleneck, the net traffic can be reduced.

**Configuring SPAN on EVC**

Complete the following steps to configure SPAN on EVC.
SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface port-channel number`
4. `[no] ip address`
5. `[no] service instance id Ethernet [service-name]`
6. `encapsulation {default|untagged|dot1q vlan-id [second-dot1q vlan-id]}`
7. `rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id | dot1ad vlan-id dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | symmetric}
8. `exit`
9. `monitor session local_span_session_number type [local | local-tx]`
10. `source {interface | service instance | vlan} {GigabitEthernet | Port-channel | TenGigabitEthernet} [rx | tx | both]`
11. `destination interface {GigabitEthernet | Port-channel | TenGigabitEthernet}`
12. `[no] shutdown`
13. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface port-channel number</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>[no] ip address</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>[no] service instance id Ethernet [service-name]</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>`encapsulation {default</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>`rewrite ingress tag {push {dot1q vlan-id</td>
</tr>
</tbody>
</table>
**Sample Configuration**

This is an example for configuring SPAN on EVC.

```
Router# enable
Router# configure terminal
Router(config)# interface port-channel 11
Router(config-if)# no ip address
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 13
Router(config-if-srv)# rewrite ingress tag push dot1q 20 symmetric
Router(config-if-srv)# exit
Router(config)# monitor session 1 type local
Router(config-mon-local)# source service instance 2 - 100 Port-channel 1 both
Router(config-mon-local)# destination interface Port-channel 3
Router(config-mon-local)# no shut
Router(config-mon-local)# end
```

**Verifying SPAN on EVC**

This section provides the commands to verify the SPAN configuration.

```
Router# show monitor session 1
Session 1
---------
Type : Local Session
Status: Admin Enabled
Source EFPs:
Both: Po1: 2-100
Destination Ports: Po3
```

```
Router# show run | section monitor
monitor session 1 type local
source service instance 2 - 100 Port-channel 1 both
destination interface Port-channel 3
```

**Troubleshooting**

For specific troubleshooting information, contact Cisco Technical Assistance Center (TAC) at this location:

Information About ERSPAN on EVC

Cisco 7600 routers support the Encapsulated Remote Switched Port Analyzer (ERSPAN) feature on a per service instance basis. It is the Ethernet Virtual Circuits (EVC) infrastructure that supports remote monitoring and troubleshooting on a per service instance basis. ERSPAN on EVC is supported on ES+ line cards.

Interception of traffic on EVC can be configured in the following ways:

- **ERSPAN on Port**: The configuration includes traffic on EVCs, switchports and routed traffic on the port.
- **ERSPAN on VLAN**: The configuration includes traffic on all EVC BDs in the box (on port or port channel) with the same VLAN for a SPAN session along with other switch ports on the same VLAN.
- **ERSPAN on EVC**: The configuration includes traffic on a given EFP or a set of EFPS (on port or port channel) for a SPAN session.

SPAN, sometimes called port mirroring or port monitoring, allows network traffic to be analyzed by a network analyzer such as a Cisco Switch Probe or other Remote Monitoring (RMON) probes. SPAN lets you monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports where the network analyzer is attached.

ERSPAN monitors traffic on multiple network devices across an IP network, and sends that traffic in an encapsulated envelope to destination analyzers. ERSPAN can be used to monitor traffic remotely.

ERSPAN monitors ingress, egress, or both kinds of network traffic. Encapsulated ERSPAN packets are routed from a host through the routed network to the destination device where they are decapsulated and forwarded to the attached network analyzer. The destination may also be on the same Layer 2 or Layer 3 network as the source.

ERSPAN consists of an ERSPAN source session, routable ERSPAN GRE encapsulated traffic, and an ERSPAN destination session.

EVCs define a Layer 2 bridging architecture that supports Ethernet services. EVC supports service convergence over Ethernet. An EVC is a conceptual service pipe within a service provider network. Metro-Ethernet Forum (MEF) defines EVC as an association between two or more user network interfaces that identifies a point-to-point or multipoint-to-multipoint path within the service provider network.

EVC is the device local object (container) for network-wide service parameters and provides one-to-many mapping from EVC to Service Instance. Its support extends to a mix of Layer 2 and Layer 3 services on the same physical port.

EVC allows routers to reach multiple intranet and extranet locations from a single physical port. Routers see subinterfaces through which they access other routers.

Bridge Domain (BD) is the Ethernet Broadcast Domain local to a device. It exists separately from VLANs. BD provides a one-to-many mapping from BD to service instances.

An Ethernet service instance is a transport-agnostic abstraction of an Ethernet service on an interface. A service instance classifies frames belonging to a particular Ethernet service. It applies features selectively to service frames, and defines forwarding actions and behavior.

Restrictions for ERSPAN on EVC Configuration

- EVC ERSPAN is effective only if the EVC is on an ES+ line card.
- EVC is not supported as ERSPAN destination.
- Egress ERSPAN packets do not undergo QoS processing.
- For egress SPAN configurations with a VLAN as the source, where the VLAN is also part of BD and switchport for the router, all traffic that goes on the VLAN is replicated and spanned.
- Many service instances having the same BD results in a mix of BDs. In such situations, for egress SPAN configurations with VLAN as source, there is random selection and spanning. All EVCs are not spanned; single EVCs are randomly selected and spanned.
- Existing implementations restrict the configuring of SPAN source as both interface and VLANs. The same restriction applies to EFP configurations. If the SPAN source is VLAN, then the interface or EFP cannot be the source.
- Encapsulation requires a dedicated tunnel. When egress monitored traffic moves out of the tunnel interface to the remote router it allows no other traffic on the router.

### Configuring the Source Session for ERSPAN on EVC

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td>Example</td>
<td>Enables the privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td></td>
<td>rtr1# enable</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>rtr1# configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>monitor session session number type erspan-source</td>
</tr>
<tr>
<td>Example</td>
<td>Configures an ERSPAN source session number, and enters the ERSPAN source session configuration mode for the session.</td>
</tr>
<tr>
<td></td>
<td>rtr1(config)#monitor session 1 type erspan-source</td>
</tr>
<tr>
<td>Step 4</td>
<td>service instance range of EFPs interface source interface</td>
</tr>
<tr>
<td>Example</td>
<td>Configures the service instance range, and specifies the sub-interface with slot and port number.</td>
</tr>
<tr>
<td></td>
<td>rtr1(config-mon-erspan-src)#source service instance 1 - 12 GigabitEthernet9/1</td>
</tr>
<tr>
<td></td>
<td>Creates a service instance (an instantiation of an EVC) on an interface, and sets the device into the service instance submode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>no shutdown</td>
</tr>
<tr>
<td>Example</td>
<td>Enables the ERSPAN session, and saves it in the running configuration. By default, the session is created in the shut state.</td>
</tr>
<tr>
<td></td>
<td>rtr1(config-mon-erspan-src)#no shutdown</td>
</tr>
<tr>
<td>Step 6</td>
<td>destination</td>
</tr>
<tr>
<td>Example</td>
<td>Enters the ERSPAN source session destination configuration mode, and associates the SPAN session number with the destination.</td>
</tr>
<tr>
<td></td>
<td>rtr1(config-mon-erspan-src)#destination</td>
</tr>
<tr>
<td>Step 7</td>
<td>ip address ip address</td>
</tr>
<tr>
<td>Example</td>
<td>Configures the ERSPAN flow destination IP address, which must also be configured on an interface on the destination router and be entered in the ERSPAN destination session configuration.</td>
</tr>
<tr>
<td></td>
<td>rtr1(config-mon-erspan-src-dst)#ip address 40.40.40.2</td>
</tr>
</tbody>
</table>
Chapter 4      Configuring Layer 1 and Layer 2 Features

Configuring the Source Session for ERSPAN on EVC

Step 8

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>origin ip address ip address</strong></td>
<td>Configures the encapsulated packet Layer 3 source address.</td>
</tr>
<tr>
<td>Example</td>
<td></td>
</tr>
<tr>
<td>rtr1(config-mon-erspan-src-dst)#origin ip address 10.10.10.10</td>
<td></td>
</tr>
</tbody>
</table>

Step 9

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>erspan-id erspan identifier</strong></td>
<td>Adds an ERSPAN ID to the session configuration. Configures the ID number used by the source and the destination sessions to identify the ERSPAN traffic. This number is unique and within the limits permitted. It is identical for the source and the destination.</td>
</tr>
<tr>
<td>Example</td>
<td></td>
</tr>
<tr>
<td>rtr1(config-mon-erspan-src-dst)#erspan-id 100</td>
<td></td>
</tr>
</tbody>
</table>

Step 10

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>end</strong></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Example</td>
<td></td>
</tr>
<tr>
<td>rtr1(config-mon-erspan-src-dst)#end</td>
<td></td>
</tr>
</tbody>
</table>

Configuration Examples for ERSPAN on EVC Source Session

rtr1(config)#monitor session 1 type erspan-source
rtr1(config-mon-erspan-src)#source service instance 1 - 12 GigabitEthernet9/1
rtr1(config-mon-erspan-src)#no shutdown
rtr1(config-mon-erspan-src)#destination
rtr1(config-mon-erspan-src-dst)#ip address 40.40.40.2
rtr1(config-mon-erspan-src-dst)#origin ip address 10.10.10.10
rtr1(config-mon-erspan-src-dst)#erspan-id 100
rtr1(config-mon-erspan-src-dst)#end

rtr1(config)#monitor session 1 type erspan-source
rtr1(config-mon-erspan-src)#source service instance 1 - 12 GigabitEthernet9/1 TX
rtr1(config-mon-erspan-src)#no shutdown
rtr1(config-mon-erspan-src)#destination
rtr1(config-mon-erspan-src-dst)#ip address 40.40.40.2
rtr1(config-mon-erspan-src-dst)#origin ip address 10.10.10.10
rtr1(config-mon-erspan-src-dst)#erspan-id 100
rtr1(config-mon-erspan-src-dst)#end

rtr1(config)#monitor session 1 type erspan-source
rtr1(config-mon-erspan-src)#source service instance 1 - 12 GigabitEthernet9/1 RX
rtr1(config-mon-erspan-src)#no shutdown
rtr1(config-mon-erspan-src)#destination
rtr1(config-mon-erspan-src-dst)#ip address 40.40.40.2
rtr1(config-mon-erspan-src-dst)#origin ip address 10.10.10.10
rtr1(config-mon-erspan-src-dst)#erspan-id 100
rtr1(config-mon-erspan-src-dst)#end

The following examples show ERSPAN on port channel configurations:

ERSPAN on Port-channel
rtr1(config)#monitor session 1 type erspan-source
rtr1(config-mon-erspan-src)#source service instance 1 - 12 port-channel 1
rtr1(config-mon-erspan-src)#no shutdown
rtr1(config-mon-erspan-src)#destination
rtr1(config-mon-erspan-src-dst)#ip address 40.40.40.2
rtr1(config-mon-erspan-src-dst)#origin ip address 10.10.10.10

Note

If the configurations exclude TX or RX, ERSPAN monitors both ingress and egress traffic.
**Configuring the Destination Session for ERSPAN on EVC**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables the privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example</td>
<td>rtr3# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example</td>
<td>rtr3# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>monitor session session number type erspan-destination</td>
<td>Configures an ERSPAN destination session number, and enters the ERSPAN destination session configuration mode for the session.</td>
</tr>
<tr>
<td></td>
<td>Example</td>
<td>rtr3(config)#monitor session 1 type erspan-destination</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>destination interface interface slot/port</td>
<td>Enters the ERSPAN destination session destination configuration mode, associates the SPAN session number with the destination, and specifies the sub-interface with slot and port number.</td>
</tr>
<tr>
<td></td>
<td>Example</td>
<td>rtr3(config-mon-erspan-dst)#destination interface GigabitEthernet7/19</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>no shutdown</td>
<td>Enables the ERSPAN session and saves it in the running configuration. By default, the session is created in the shut state.</td>
</tr>
<tr>
<td></td>
<td>Example</td>
<td>rtr3(config-mon-erspan-dst)#no shutdown</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>source</td>
<td>Enters the ERSPAN destination session source configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example</td>
<td>rtr3(config-mon-erspan-dst)#source</td>
</tr>
</tbody>
</table>
### LACP Support for EVC Port Channel

An Ethernet link bundle or port-channel is an aggregation of up to eight physical Ethernet links to form a single logical link for L2/L3 forwarding. Bundled Ethernet ports are used to increase the capacity of the logical link and provide high availability and redundancy. The EVC EtherChannel feature provides support for EtherChannels on Ethernet Virtual Connection Services (EVCS) service instances.

For more information on EtherChannels, and how to configure EtherChannels on Layer 2 or Layer 3 LAN ports, see "Configuring EtherChannels" at http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/channel.html.

---

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>ip address ip address</strong>&lt;br&gt;Example: <code>rtr3(config-mon-erspan-dst-src)#ip address 40.40.40.2</code>&lt;br&gt;Configures the ERSPAN flow destination IP address, which must also be configured on an interface on the destination router, and entered in the ERSPAN destination session configuration.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>erspan-id erspan identifier</strong>&lt;br&gt;Example: <code>rtr3(config-mon-erspan-dst-src)#erspan-id 100</code>&lt;br&gt;Adds an ERSPAN ID to the session configuration. Configures the ID number used by the source and destination sessions to identify the ERSPAN traffic. This number is unique and within the prescribed limits. It is identical for the source and the destination.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>end</strong>&lt;br&gt;Example: <code>rtr3(config-mon-erspan-dst-src)#end</code>&lt;br&gt;Exits the configuration mode.</td>
</tr>
</tbody>
</table>

### ERSPAN on EVC: Destination Session Configuration Example

```
  rtr3(config)#monitor session 1 type erspan-destination
  rtr3(config-mon-erspan-dst)#destination interface GigabitEthernet7/19
  rtr3(config-mon-erspan-dst)#no shutdown
  rtr3(config-mon-erspan-dst)#source
  rtr3(config-mon-erspan-dst-src)#ip address 40.40.40.2
  rtr3(config-mon-erspan-dst-src)#erspan-id 100
  rtr3(config-mon-erspan-dst-src)#end
```

### Verification of ERSPAN on EVC Configuration

Use the following command to verify the ERSPAN on EVC configurations:

```
  show monitor session all
```

### Verification Example for ERSPAN on EVC

```
  rtr1#show monitor session all
  Session 1
  -----------
  Type : ERSPAN Destination Session
  Status : Admin Disabled
  Source IP Address : 1.1.1.1
  Source ERSPAN ID : 100
```
The EVC EtherChannel feature supports MPBE, local connect, and xconnect service types. IEEE 802.3ad/Link Aggregation Control Protocol (LACP) provides an association of port-channels. The LACP support for EVC Port Channel feature supports service instances over bundled Ethernet links.

Ethernet flow points (EFPs) are configured under a port-channel. The traffic, carried by the EFPs, is load-balanced across member links. EFPs under a port-channel are grouped and each group is associated with one member link. Ingress traffic for a single EVC can arrive on any member of the bundle. All egress traffic for an EFP uses only one of the member links. Load balancing is achieved by grouping EFPs and assigning them to a member link.

The scalability for a link-bundling EVC is 16000 per chassis. Port Channel EVC scalability for ES+ line cards is dependent on the same factors as EVCs configured under physical interfaces, with the number of member links and their distribution across the NPU as an additional parameter. EVC port-channel QoS leverages EVC QoS infrastructure. For more information on the scalable values, see Restrictions and Usage Guidelines, page 4-24.

**Restrictions and Usage Guidelines**

When configuring EVC EtherChannel, follow these restrictions and usage guidelines:

- All member links of the port-channel are on Cisco 7600-ES+ line cards.
- Only bridge-domain, xconnect, connect EVCs, and IP subinterfaces are allowed over the port-channel interface. You cannot apply a switchport and EVC configuration under the same port-channel interface.
- If you configure a physical port as part of a channel group, you cannot configure EVCs under that physical port.
- A physical port that is part of an EVC port-channel cannot have switchport configuration.
- You can apply QoS policies under EVCs on a port-channel with the exception that ingress microflow policing is not supported. For more information on configuring QoS with EVCs, see Configuring QoS, page 7-1.
- You cannot use the **bandwidth percent** or **police percent** commands on EVC port-channels in flat policy-maps or in parent of HQoS policy-maps.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface port-channel`
4. `[no] ip address`
5. `service instance id Ethernet [service-name]`
6. `encapsulation dot1q vlan-id`
7. `rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} } symmetric`
8. `[no] bridge-domain bridge-id`
9. `interface gigabitethernet slot/port`
10. `channel-protocol {lacp | pagp}`
11. **channel-group channel-group-number mode** \{active | on | passive\}

**Note**

The `channel-group` command options are applicable when configuring port-channel over EVC and the options active/passive are applicable when configuring port-channel over EVC with LACP.

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
  - Enter your password if prompted.  
  
  **Example:**  
  ```console`  
  Router# enable  
  ``` |
| Step 2 | `configure terminal` | Enters global configuration mode.  
  
  **Example:**  
  ```console`  
  Router# configure terminal  
  ``` |
| Step 3 | `interface port-channel number` | Creates the port-channel interface.  
  
  **Example:**  
  ```console`  
  Router(config)# interface port-channel 12  
  ``` |
| Step 4 | `[no] ip address` | Assigns a subnet mask to the EtherChannel.  
  
  **Example:**  
  ```console`  
  Router(config-if)# no ip address  
  ``` |
| Step 5 | `[no] service instance id Ethernet [service-name]` | Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.  
  
  **Example:**  
  ```console`  
  Router(config-if)# service instance 101 ethernet  
  ``` |
| Step 6 | `encapsulation dot1q vlan-id` | Defines the matching criteria to be used to map ingress dot1q frames on an interface to the appropriate service instance.  
  
  **Example:**  
  ```console`  
  Router(config-if-srv)# encapsulation dot1q 13  
  ``` |
### LACP Support for EVC Port Channel

#### Command and Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>rewrite ingress tag {push (dot1q vlan-id</td>
<td>dot1q vlan-id second-dot1q vlan-id</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if-srv)# rewrite ingress tag push dot1q 20 symmetric</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>[no] bridge-domain bridge-id</td>
<td>Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if-srv)# bridge-domain 12</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>interface gigabitethernet slot/port</td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.</td>
</tr>
<tr>
<td></td>
<td>Example: Router (config) # interface gig 5/1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>channel-protocol {lacp</td>
<td>pagp}</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if)# channel-protocol lacp</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>channel-group channel-group-number mode {active</td>
<td>on</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if)# channel-group 5 mode active</td>
<td></td>
</tr>
</tbody>
</table>

---

**Examples**

In this example, a single port-channel interface is created with three possible member links from slots 1 and 2:

```bash
Router# enable
Router# configure terminal
Router(config)# interface Port-channel5
Router(config-if)# no ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 350
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 350
!
Router(config-if)# service instance 2 ethernet
Router(config-if-srv)# encapsulation dot1q 400
```
This is a typical QoS configuration.

This is configuration for LACP over a configured EVC port-channel, under an interface:

This is a port-channel configuration:

This is a member links configuration:
Router# enable
Router# configure terminal
Router(config-if)# interface GigabitEthernet 3/12
Router(config-if)# mtu 9216
Router(config-if)# no ip address
Router(config-if)# lacp rate fast
Router(config-if)# channel-protocol lacp
Router(config-if)# channel-group 102 mode active

Verification

Use these commands to verify EVC configuration.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ethernet service evc [id evc-id</td>
<td>interface interface-id] [detail]</td>
</tr>
<tr>
<td>Router# show ethernet service instance interface-id port-channel number [summary]</td>
<td>Displays the summary of all the EVCs configured within the interface.</td>
</tr>
<tr>
<td>Router# show ethernet service instance [id instance-id interface interface-id</td>
<td>interface interface-id] [detail]</td>
</tr>
<tr>
<td>Router# show ethernet service interface [interface-id] [detail]</td>
<td>Displays information in the Port Data Block (PDB).</td>
</tr>
</tbody>
</table>

Use the following commands to verify LACP over EVC

Router# show etherchannel 15 port-channel | Displays details for port-channel 15. This command is common to EVC port-channel, switchport port-channel, and Layer 3 port-channel. |

Troubleshooting

For information on troubleshooting LACP support for EVC Port Channel feature, see Table 4-6 on page 4-52.
Configuring Layer 2 Access Control Lists (ACLs) on an EVC

ACLs (Access Control Lists) perform the following tasks:

- Apply security and QoS at the interface, sub-interface, and service levels.
- Filter the packets in a modular manner.

You can use a collection of sequential ACL rules to filter network traffic. Though the ACLs are applied on a network interface, you can use this feature to apply Layer 2 on different EVCs. Table 4-7 maps the supported layers with their parameters and Table 4-8 lists the commands used to activate the Layer 2 ACLs.

Table 4-7  Mapping between the ACL supported layers to the parameters

<table>
<thead>
<tr>
<th>Layer</th>
<th>Based on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2</td>
<td>• MAC source and destination</td>
</tr>
</tbody>
</table>

Table 4-8  ACL commands

<table>
<thead>
<tr>
<th>Layer</th>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2</td>
<td>Create a Layer 2 Access List</td>
<td><code>mac access-list extended {aclname}</code></td>
</tr>
<tr>
<td></td>
<td>Apply an Access list within</td>
<td><code>mac access-group {aclname} in</code></td>
</tr>
<tr>
<td></td>
<td>the EVC</td>
<td></td>
</tr>
</tbody>
</table>

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines when you configure ACLs on a EVC:

- A Layer 2 ACL is supported only on the ingress.
- You can apply a single ACL to more than one EFP.
- If a Layer 2 ACL is applied to an EFP (Ethernet Flow Point) with a Layer 2 ACL, the new ACL replaces the previous ACL.
- A Layer 2 ACL configuration applied on the EVC interface should contain the source MAC address, destination MAC address, and the address mask.
- You can apply a maximum of 256 unique ACLs on all the EVCs.
- Maximum number of 16 ACEs (Access Control Elements) per ACL are supported.
- The counters are supported per ACL per EVC.
- Cisco IOS Release 15.1(1)S supports EVC port-channels.

Creating a Layer 2 Access Control List

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `mac access-list extended {aclname} {permit | deny} {host a.b.c host x.y.z}`
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 mac access-list extended aclname (permit</td>
<td>Creates a Layer 2 Access List on the selected interface.</td>
</tr>
<tr>
<td>deny) (host a.b.c host x.y.z)</td>
<td>Creates a Layer 2 Access List on the selected interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Creates a Layer 2 Access List on the selected interface.</td>
</tr>
<tr>
<td>me7600-5(config)#mac access-list extended test-l2-acl</td>
<td>Creates a Layer 2 Access List on the selected interface.</td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>

Applying a Layer 2 Access Control List

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet type/ slot/port [subinterface-number] or interface tengigabitethernet type/ slot/port [subinterface-number]
4. [no] service instance id {Ethernet}/
5. encapsulation dot1q vlan id
6. mac access-group aclname in
7. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |

**Example:**  
Router> enable

| **Step 2** configure terminal | Enters global configuration mode. |

**Example:**  
Router# configure terminal

| **Step 3** interface gigabitethernet type/ slot/port  
[ subinterface-number ]  
or  
interface tengigabitethernet type/  
slot/port [ subinterface-number ] | Specifies the gigabit ethernet or the ten gigabit ethernet interface to configure, where:  
- slot/subslot/port—Specifies the location of the interface.  
- subinterface-number—(Optional) Specifies a secondary interface (sub-interface) number. |

**Example:**  
Router(config)# interface gigabitethernet 4/0/0

| **Step 4** [ no ] service instance id { Ethernet [ service-name ] } | Creates a service instance on an interface and sets the device to the config-if-srv configuration mode. |

**Example:**  
Router(config-if)# service instance 101 ethernet

| **Step 5** encapsulation dot1q vlan id | Defines the matching criteria to map ingress dot1q frames on an interface to the appropriate service instance.  
**Note** Use the `encapsulation dot1q default` command to configure the default service instance on a port. Use the `encapsulation dot1q untagged` command to map the untagged ethernet frames on an ingress interface to a service instance. |

**Example:**  
Router(config-if-srv)# encapsulation dot1q 5

| **Step 6** mac access-group aclname in | Applies a L2 ACL on the selected EVC.  
**Note** L2 ACL displays only positive permit and deny counts. |

**Example:**  
me7600-5(config-if-srv)# mac access-group test-l2-acl in

| **Step 7** exit | Exits the configuration mode. |

### Examples

You can view the ACL counters for an EVC as shown in this example:

```
LLB-India-7#sh ethernet service instance id 1 int gig3/0/0 detail
Service Instance ID: 1
L2 ACL (inbound): l2acl
Associated Interface: GigabitEthernet3/0/0
Associated EVC: test
```

<<<<

12acl
DHCP Snooping with Option-82 on EVC

DHCP snooping determines whether traffic sources are trusted or untrusted. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, DHCP snooping filters messages traffic from untrusted sources.

To do this, DHCP snooping dynamically builds and maintains the DHCP snooping database using information extracted from intercepted DHCP messages. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts connected through trusted interfaces.

Each entry in the DHCP snooping database includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.

Additionally, the DHCP Snooping with Option-82 feature can centrally manage the IP address assignments for a large number of subscribers. When this feature is enabled on the router, a subscriber device is identified by the router port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access router and are uniquely identified.

However, EVCs require additional information. If each EVC on an interface is mapped to a single VPN, it would be possible to use the internal VLAN to identify the path for reply packets. However, because multiple EVCs with different encapsulations can map to the same VPN, it is necessary to use the actual EVC encapsulation to distinguish between EVCs.

The DHCP Snooping with Option-82 on EVC feature allows the user to provide this additional information required for EVC-enabled interfaces. This information is inserted into the option 82 and is also stored in the binding table for retrieval by other services.

Use the `ip dhcp snooping information option allow-untrusted` command to enable the switch to accept incoming DHCP snooping packets with option 82 information from the edge switch. DHCP option 82 data insertion is enabled by default. Accepting incoming DHCP snooping packets with option 82 information from the edge switch is disabled by default.

Use the `ip dhcp relay information option subscriber-id` command to configure a subscriber string for an EVC that can be inserted into the option 82 field along with other information when relaying the DHCP packets to the server. The server can parse the option 82 information to match the subscriber string and act accordingly. The subscriber string configured for an EVC will not be stored in the binding table and is only used when sending DHCP packets to the server by inserting into the option 82 field.

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines while you configure DHCP Snooping with Option-82:

- An EVC with multiple encapsulations is not supported.
- The following EVCs are supported on the same interface and bridge-domain:
  - dot1q encapsulation
  - QinQ encapsulation
  - Untagged encapsulation
- 4000 EVCs are supported per port.
- 32000 EVCs are supported per router.
- Multiple EVCs are supported on the same port, all having the same or different bridge domains.
- Multiple EVCs are supported on different ports, all having the same or different bridge domains.
- With Cisco IOS Release 12.2(33)SRE, DHCP snooping with Option 82 is supported on EVC port-channels.
- DHCP snooping is not supported with lag NNI VPLS core.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/port or interface tengigabitethernet slot/port or interface port-channel number
4. [no] ip address
5. negotiation { forced | auto }
6. service instance id Ethernet [ service-name ]
7. encapsulation dot1q vlan-id
8. rewrite ingress tag { push { dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id } | pop {1 | 2} | translate { 1-to-1 { dot1q vlan-id | dot1ad vlan-id } | 2-to-1 dot1q vlan-id | dot1ad vlan-id } | 1-to-2 { dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id } | 2-to-2 { dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id } } symmetric
9. ip dhcp relay information option subscriber-id value
10. [no] bridge-domain bridge-id
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt;Example: Router# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;Example: Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>interface gigabitethernet slot/subslot/port[/subinterface-number]</strong>&lt;br&gt;or&lt;br&gt;<strong>interface tengigabitethernet slot/subslot/port[/subinterface-number]</strong>&lt;br&gt;or&lt;br&gt;<strong>interface port-channel number</strong>&lt;br&gt;Example: Router(config)# interface gigabitethernet 4/1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>no ip address</strong>&lt;br&gt;Example: Router# Router(config-if)# no ip address</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**negotiation {forced</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>[no] service instance id Ethernet [service-name]</strong>&lt;br&gt;Example: Router(config-if)# service instance 101 ethernet</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>encapsulation dot1q vlan-id</strong>&lt;br&gt;Example: Router(config-if-srv)# encapsulation dot1q 13</td>
</tr>
</tbody>
</table>
**Example**

This example shows a typical configuration on the relay agent and the server. This is a configuration on the relay agent:

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet8/1
Router(config-if)# no ip address
Router(config-if)# negotiation auto
Router(config-if)# service instance 2 ethernet
Router(config-if-srv)# encapsulation dot1q 2
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
   ip dhcp relay information option subscriber-id 11
Router(config-if-srv)# bridge-domain 100
```

```
Router(config)# interface Vlan100
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip helper-address global 20.0.0.2
Router(config-if)# ip helper-address 20.0.0.2
```

```
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# ip dhcp snooping packets
Router(config-if)# ip address 20.0.0.1 255.255.255.0
Router(config-if)# negotiation auto
```

This is the configuration on the server:

```
Router# enable
Router# configure terminal
```

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> rewrite ingress tag {push (dot1q vlan-id</td>
<td>dot1q vlan-id second-dot1q vlan-id</td>
</tr>
<tr>
<td><strong>Step 9</strong> ip dhcp relay information option subscriber-id value</td>
<td>Configures a subscriber string that uniquely identifies the interface from where the DHCP packets originate.</td>
</tr>
<tr>
<td><strong>Step 10</strong> [no] bridge-domain bridge-id</td>
<td>Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.</td>
</tr>
</tbody>
</table>
Router(config)# interface GigabitEthernet 1/1
Router(config-if)# ip address 20.0.0.2 255.255.255.0
Router(config-if)# negotiation auto
Router(config-if)# end

Router(config)# ip dhcp pool pool1
Router(config)# network 10.0.0.0 255.255.0.0
   lease 2
Router(config)# update arp
class C1
   address range 10.0.0.2 10.0.0.10
class C2
   address range 10.0.0.11 10.0.0.20
!
Router(config)# ip dhcp pool pool2
Router(config)# network 11.0.0.0 255.255.0.0 lease 2
!
Router(config)# ip dhcp pool pool3
   vrf vrf1
Router(config)# network 10.0.0.0 255.255.255.0 lease 0 0 2
!

ip dhcp class C1 <--------Class C1 maps to the subscriber-id string aabb11.
   relay agent information
   relay-information hex 00000000000000000000000000000006616162623131 mask
                       ffffffffffffffffffffffffffffffff0000000000000
!
ip dhcp class C2
   relay agent information
   relay-information hex 00000000000000000000000000000006313162626161 mask
                       ffffffffffffffffffffffffffffffff0000000000000

Verification

Use this commands to verify operation.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ip dhcp snooping</td>
<td>Displays all VLANs (both primary and secondary) that have DHCP snooping enabled.</td>
</tr>
<tr>
<td>Router# show ip dhcp snooping binding</td>
<td>Checks the DHCP snooping database.</td>
</tr>
</tbody>
</table>

Troubleshooting

Table 4-9 provides the troubleshooting solutions for the DHCP Snooping feature.
DHCP Snooping Over p-mLACP

The Dynamic Host Configuration Protocol (DHCP) snooping over a pseudo-multichassis Link Aggregate Control Protocol (p-mLACP) feature synchronizes the DHCP snooping database between the Point of Attachments (PoAs) in a network. The synchronization of the DHCP database allows the multicast traffic to flow with the least interruption when the p-mLACP fails. This feature uses the Interchassis Communication Protocol (ICCP) to synchronize the DHCP snooping database with the peer PoAs to provide multi-chassis redundancy. When the multi-chasss Link Aggregation (mLAG) transitions from a standby VLAN to the active VLAN on a chassis, this feature facilitates the state

**Table 4-9  Troubleshooting Scenarios for DHCP Snooping feature**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP snooping database is not storing any bindings</td>
<td>Complete the following steps to verify and troubleshoot:</td>
</tr>
<tr>
<td></td>
<td>1. Use the <code>show ip dhcp snooping binding</code> command to check whether there are non-zero bindings built on the binding table.</td>
</tr>
<tr>
<td></td>
<td>2. The <code>show ip dhcp snooping binding</code> command displays the <code>total number of bindings</code> as a non-zero value. If not, check whether the DHCP snooping database agent is configured correctly. If no bindings exist, it implies that they were never built or the lease expired. Reconfigure the bindings with a longer lease period. If the lease time is configured as maximum (4294967295 seconds effective from 12.2(33) SRD), the bindings do not expire.</td>
</tr>
<tr>
<td></td>
<td>3. Use the <code>ip dhcp snooping database</code> command to check if the DHCP snooping database agent is configured correctly and is currently running.</td>
</tr>
<tr>
<td>Bindings are not getting stored in the database agent</td>
<td>Read the database agent file to check if bindings are stored in that file. If not, go to Step 3 of the previous solution. If there is at least one binding stored in the database file, it implies that the database agent is working fine.</td>
</tr>
<tr>
<td>DHCP snooping is not active on the router</td>
<td>DHCP snooping is active on the router only when it is configured globally and on at least one interface VLAN. Check if the <code>ip dhcp snooping</code> command exists in the running and global configuration modes, and at least on one VLAN interface. If not, configure the feature as described in Configuring Layer 2 Access Control Lists (ACLs) on an EVC, page 4-66.</td>
</tr>
<tr>
<td></td>
<td>If the configurations exist, use the <code>debug ip dhcp snooping packets</code> command to check whether or not DHCP packets are being exchanged between the DHCP server and the client. If yes, proceed to Step 3 listed in the solution for “DHCP snooping database is not storing any bindings” problem. If not, check the configurations for the DHCP server and client and whether all the connections to the DHCP relay agent are fine.</td>
</tr>
<tr>
<td></td>
<td>If the problem persists, contact TAC.</td>
</tr>
</tbody>
</table>
change with minimal traffic disruption in the network. A system configured with DHCP snooping creates a DHCP snooping database, which contains DHCP snooping entries (MAC/IP bindings) learnt from the different VLANs.

The DHCP snooping binding data is added in the active supervisor after successfully synchronizing the snooping information between the local standby and remote PoAs (active and standby supervisor PoA).

Note

For more information on pmLACP and p-mLACP failure, see Pseudo MLACP Support on Cisco 7600 section in the Cisco 7600 Series ES+ and ES+T Line Card Configuration Guide.

DHCP Snooping State Synchronization

The DHCP snooping state synchronization involves these steps:

0. The active PoA synchronizes the DHCP snooping binding tables with the standby PoA.
1. The standby PoA uses the synchronized DHCP binding information for IP source guard (IPSG) and Dynamic ARP Inspection (DAI).
2. On switchover, the standby EFP becomes active and any spoofed ARP, MAC or IP traffic is dropped by the new Active PoA.

Restrictions for DHCP Snooping over p-mLACP

Following restrictions apply for the DHCP Snooping over p-mLACP feature:

- The manual load-balance VLAN list and LAG configuration should be same on both the PoAs.
- The bridge-domain configured under a p-mLACP port-channel EVC should not be part of any other non-pmLACP interfaces.
- For proper DHCP snooping database synchronization, ensure that the ICRM link is up.
- All the PoAs should be configured as p-mLACP peers to enable DHCP snooping database synchronization.
- It is recommended that all the PoAs should be configured for non-revertive mode.
- During the mLACP failures A, B, C, and E, the database entries are not lost. In case of p-mLACP failure D, the database entries are lost but they are restored after synchronization with the peer PoA through the ICRM link.
- The maximum number of DHCP Snooping entries supported per PoA is 20000; 10000 entries on the active VLAN on the active PoA and 10000 entries synchronized from another PoA through the ICCP link.
- This feature is supported on the ES20 and ES+ line cards in the access mode only.
- This feature is supported on both SUP720 and RSP720 (1 GHz & 10 GHz).
- For the Virtual Private Lan Service (VPLS)-decoupled mode, all the Ethernet Flow Points (EFPs) participating in a bridge-domain should have the outer tag VLAN range set to either primary or secondary VLANs, but not both.
- If an EFP is deleted from a PoA, you should remove it from the all the peer PoAs.
- While adding EFPs to a PoA, add the standby EFP before adding the active EFP.
- IP FRR functionality is not supported with p-mLACP.
Pseudo-Multichassis LACP (p-mLACP) IGMP Snooping State Synchronization

Note

All the p-mLACP restrictions also apply to this feature.

Table 4-10 lists the scalability numbers for DHCP Snooping state synchronization:

Table 4-10  Scalability Numbers for p-mLACP DHCP Snooping State Synchronization

<table>
<thead>
<tr>
<th>Feature</th>
<th>Per PoA</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP snooping entries</td>
<td>20000</td>
</tr>
</tbody>
</table>

Troubleshooting Tips

Table 4-11 lists the commands to troubleshoot the p-mLACP DHCP Snooping State Synchronization.

Table 4-11  Troubleshooting Scenarios

<table>
<thead>
<tr>
<th>Command</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip dhcp snooping event</td>
<td>Use this command to enable the debugging of the events involved in DHCP snooping.</td>
</tr>
<tr>
<td>debug ip dhcp snooping packet</td>
<td>Use this command to display the debugging messages for DHCP snooping.</td>
</tr>
<tr>
<td>show ip dhcp snooping multi-chassis</td>
<td>Use this command to display status of bulk synchronization.</td>
</tr>
</tbody>
</table>

Pseudo-Multichassis LACP (p-mLACP) IGMP Snooping State Synchronization

The pseudo-multichassis Link Aggregate Control Protocol (p-mLACP) Internet Group Management Protocol (IGMP) Snooping State Synchronization feature synchronizes the IGMP snooping database between the Point of Attachments (PoAs) in a network. The synchronization of the IGMP database allows the multicast traffic to flow with the least interruption when an mLACP fails. The p-mLACP IGMP snooping function uses the Interchassis Communication Protocol (ICCP) to synchronize the IGMP snooping database with the peer PoAs. When the mLAG transitions from a standby VLAN to the active VLAN on a chassis, this feature facilitates the state change with minimal traffic disruption in the network.

Note

For more information on pmLACP and p-mLACP failure, see Pseudo MLACP Support on Cisco 7600 section in the Cisco 7600 Series ES+ and ES+T Line Card Configuration Guide.

IGMP Snooping State Synchronization

The p-mLACP IGMP Snooping state synchronization involves these steps:
POA creates snooping entries for its active VLANs based IGMP reports and the snooping entries are synchronized to the peer POA using ICCP, where this information corresponds to the standby VLANs on peer POA.

The peer POA processes the ICCP messages received from the other POA, and pre-programs the multicast forwarding table based on the received IGMP information.

When p-mLACP fails (A, B, C, D, E) on one of the POA, the peer POA moves its standby VLANs to active and triggers IGMP reports towards the Designated Router/mrouter based on the IGMP information received via ICCP for these VLANs.

Next, the peer POA starts forwarding multicast data traffic based on pre-programmed multicast forwarding table without any delay, enabling fast convergence.

Figure 4-4 shows the basic p-mLACP IGMP Snooping State Synchronization process.

**Restrictions for p-mLACP IGMP Snooping State Synchronization**

Following restrictions apply for the p-mLACP IGMP Snooping State Synchronization feature:

- The maximum rate supported is 1000 IGMP joins per second.
- The maximum number of IGMP Snooping entries supported per PoA is 10000.
- IGMP version 2 is supported. IGMP version 3 is not supported.
- This feature is supported on the ES20 and ES+ line cards in the access mode only.
- This feature is supported on both SUP720 and RSP720 (1 GHz & 10 GHz).
- For the Virtual Private Lan Service (VPLS)-decoupled mode, all the Ethernet Flow Points (EFPs) participating in a bridge-domain should have the outer tag VLAN range set to either primary or secondary VLANs, but not both.
- If an EFP is deleted from a PoA, you should remove it from the all the peer PoAs.
- While adding EFPs to a PoA, add the standby EFP before adding the active EFP.
- IP FRR functionality is not supported with p-mLACP.
- IGMP Snooping is not supported with Hierarchical Virtual Private LAN Service (H-VPLS) and MAC Tunneling Protocol (MTP) scenarios and topologies.

Table 4-12 lists the scalability numbers for IGMP snooping state synchronization.
### Pseudo-Multichassis LACP (p-mLACP) IGMP Snooping State Synchronization

#### Table 4-12 Scalability Numbers for p-mLACP IGMP Snooping State Synchronization

<table>
<thead>
<tr>
<th>Feature</th>
<th>Per PoA</th>
<th>Desirable per PoA</th>
<th>Per RG</th>
</tr>
</thead>
<tbody>
<tr>
<td>p-mLACP IGMP snooping state synchronization</td>
<td>10K</td>
<td>20K</td>
<td>10K</td>
</tr>
</tbody>
</table>

#### Note
All p-mLACP restrictions also apply to IGMP Snooping over p-mLACP feature.

### Troubleshooting Tips

Table 4-13 lists the troubleshooting solutions for the p-mLACP IGMP Snooping State Sync implementation.

#### Table 4-13 Troubleshooting Scenarios

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP snooping database is empty on the PoA.</td>
<td>Complete these steps to verify and troubleshoot:</td>
</tr>
<tr>
<td></td>
<td>1. Use the <code>show mac-address-table multicast igmp-snooping</code> command to check for incomplete snooping entries. If the entries are incomplete, see the problem definition and solution explained in the next row</td>
</tr>
<tr>
<td></td>
<td>2. If the output from the <code>show mac-address-table multicast igmp-snooping</code> command is empty, check if the IGMP snooping is enabled on the router. Enable the IGMP snooping, if disabled.</td>
</tr>
<tr>
<td>IGMP Snooping database shows incomplete snooping entries</td>
<td>If incomplete entries are displayed in the <code>show mac-address-table multicast igmp-snooping</code> command output, complete these steps:</td>
</tr>
<tr>
<td></td>
<td>1. Check whether the incomplete entries are specific to the active VLANs or the standby VLANs.</td>
</tr>
<tr>
<td></td>
<td>2. If the incomplete entries correspond to an active VLAN, verify the configuration.</td>
</tr>
<tr>
<td></td>
<td>3. If the incomplete entries correspond to a standby VLAN, check the corresponding VC states using the <code>show mpls l2transport vc</code> command. VC state should be in <code>UP/STANDBY</code> state, not in the <code>DOWN</code> state.</td>
</tr>
<tr>
<td></td>
<td>4. Use the <code>show ip ig snooping mrouter</code> command output to verify if the mrouter port is configured properly for the affected VLAN.</td>
</tr>
</tbody>
</table>
IP Source Guard for Service Instance

An IP source guard filters a source IP address on a layer 2 port and prevents malicious hosts from impersonating a legitimate host. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted layer 2 access ports.

Initially, all IP traffic on the service instance is blocked except for DHCP packets that are captured by DHCP snooping. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, the IP source guard for service instance feature automatically creates an access control list (ACL) to permit that traffic. Traffic from other hosts is denied. This filtering limits the ability of a host to attack the network by claiming the IP address of a neighbor host.

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines while configuring IP source guard for a service instance:

- The number of ACLs and ACEs that can be configured as part of IP source guard are bounded by the hardware resources on the line card.
- The IP source guard is meant to verify host source IP and MAC information. Only ingress traffic is filtered. It is not applicable to egress direction.
- The IP source guard is not effective for software forwarded packets. When a non-recoverable TCAM exception occurs for the IP source guard, the IP filtering is not effective and packets are permitted.
- The IP source guard is not supported on subinterfaces.
- The IP source guard is supported only on ES+ line cards.
- IP source guard is supported on port-channel service instances effective from Cisco IOS release 15.1(2)S.

Configuring IP Source Guard for a Service Instance

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/port
   or
   interface tengigabitethernet slot/port
   or
   interface port-channel number
4. [no] ip address
5. service instance id ethernet [service-name]
6. encapsulation dot1q vlan-id
7. rewrite ingress tag {push dot1 vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id | pop 1 | 2} | translate 1-to-1 dot1q vlan-id dot1ad vlan-id | 2-to-1 dot1q vlan-id dot1ad vlan-id | 1-to-2 dot1q vlan-id second-dot1q vlan-id dot1ad vlan-id dot1q vlan-id | 2-to-2 dot1q vlan-id second-dot1q vlan-id dot1ad vlan-id dot1q vlan-id} symmetric
### Note
To distinguish if the packet is DHCP, all tags must be **pop, push** and **translate** are not supported with the IP source guard for service instance feature.

8. `ip verify source vlan dhcp-snooping [port-security]`
9. `[no] bridge-domain bridge-id`
10. `exit`
11. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode. If prompted, enter your password.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>interface gigabitethernet slot/port</code> or <code>interface tengigabitethernet slot/port</code> or <code>interface port-channel number</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface gigabitethernet 4/1</td>
</tr>
<tr>
<td></td>
<td>Specifies the interface to configure.</td>
</tr>
<tr>
<td></td>
<td>- <strong>slot/port</strong> - Specifies the location of the interface.</td>
</tr>
<tr>
<td></td>
<td>- <strong>number</strong> - Specifies the port channel interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>[no] ip address</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# no ip address</td>
</tr>
<tr>
<td></td>
<td>Removes an IP address or disable IP processing.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>[no] service instance id ethernet {service-name}</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# service instance 101 ethernet</td>
</tr>
<tr>
<td></td>
<td>Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>encapsulation dot1q vlan-id</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-srv)# encapsulation dot1q 13</td>
</tr>
<tr>
<td></td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
</tbody>
</table>
### Example

This example shows how to configure IP source guard for a service instance with single tag (Dot1Q) encapsulation:

```bash
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet7/1
Router(config-if)# no ip address
Router(config-if)# service instance 71 ethernet
Router(config-if-srv)# encapsulation dot1q 71
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# ip verify source vlan dhcp-snooping
Router(config-if-srv)# bridge-domain 10
```
This is example shows how to configure IP source guard for a service instance with double tag (QinQ) encapsulation.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet7/1
Router(config-if)# no ip address
Router(config-if)# service instance 71 ethernet
Router(config-if-srv)# encapsulation dot1q 71 second-dot1q 100
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# ip verify source vlan dhcp-snooping
Router(config-if-srv)# bridge-domain 10
```

This example shows how to configure IP source guard for a service instance with untagged encapsulation.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet7/1
Router(config-if)# no ip address
Router(config-if)# service instance 71 ethernet
Router(config-if-srv)# encapsulation untagged
Router(config-if-srv)# ip verify source vlan dhcp-snooping
Router(config-if-srv)# bridge-domain 10
```

This example shows how to configure IP source guard for a service instance with default encapsulation.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet7/1
Router(config-if)# no ip address
Router(config-if)# service instance 71 ethernet
Router(config-if-srv)# encapsulation default
Router(config-if-srv)# ip verify source vlan dhcp-snooping
Router(config-if-srv)# bridge-domain 10
```

This example shows how to configure IP source guard for a service instance with single tag encapsulation on a port-channel interface.

```
Router# enable
Router# configure terminal
Router(config)# interface port-channel 2
Router(config-if)# no ip address
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# ip verify source vlan dhcp-snooping
Router(config-if-srv)# bridge-domain 10
```

**Verification**

Use the `show ip verify source interface` to verify the configuration:

```
router# show ip verify source interface gi5/1 efp_id 10
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan        EFP
ID
---------    -----------    -----------      ---------------     -----------------  ----------
Gi5/1 ip-mac       active           123.1.1.1        00:0A:00:0A:00:0A  100      10
```

```
router# show ip verify source interface gi5/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address          Vlan        EFP
ID
---------    -----------    -----------      ---------------          ----------  ----------
```

This example shows how to configure IP source guard for a service instance with single tag encapsulation on a port-channel interface.
Configuring MST on EVC Bridge Domain


This section describes how to configure MST on EVC Bridge Domain. It contains these topics:

- Overview of MST and STP, page 4-84
- Overview of MST on EVC Bridge Domain, page 4-84
- Restrictions and Usage Guidelines, page 4-85
- Examples, page 4-87

Troubleshooting

Table 4-14 provides troubleshooting solutions for the IP source guard feature.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVC disabled in IP source guard</td>
<td>Use the [no] ip verify source vlan dhcp-snooping port-security command in the service instance configuration mode to verify the IP source guard information. port-security is an optional keyword to indicate that the source MAC address filter should be applied with the source IP address. Share the output with TAC to troubleshoot further.</td>
</tr>
</tbody>
</table>
| DHCP snooping failures                 | 1. Verify whether or not the issues are specific to DHCP snooping or IP source guard. Use the show ip dhcp snooping binding command to check the DHCP snooping bindings on the RP. If the expected entry is missing on the RP, debug the DHCP snooping sessions and share the output with TAC.  
2. If the entry is displayed on the route processor, but not on the line card, use the dhcp snooping ipc debug command on the RP to debug failures related to DHCP snooping entries. If the issue persists, contact TAC. |
Overview of MST and STP

Spanning Tree Protocol (STP) is a Layer 2 link-management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

Cisco 7600 series routers use STP (the IEEE 802.1D bridge protocol) on all VLANs. By default, a single instance of STP runs on each configured VLAN (provided you do not manually disable STP). You can enable and disable STP on a per-VLAN basis.

MST maps multiple VLANs into a spanning tree instance, with each instance having a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning tree instances required to support a large number of VLANs. MST improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

For routers to participate in MST instances, you must consistently configure the routers with the same MST configuration information. A collection of interconnected routers that have the same MST configuration comprises an MST region. For two or more routers to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same MST name.

The MST configuration controls the MST region to which each router belongs. The configuration includes the name of the region, the revision number, and the MST VLAN-to-instance assignment map.

A region can have one or multiple members with the same MST configuration; each member must be capable of processing RSTP bridge protocol data units (BPDUs). There is no limit to the number of MST regions in a network, but each region can support up to 65 spanning tree instances. Instances can be identified by any number in the range from 0 to 4094. You can assign a VLAN to only one spanning tree instance at a time.

For additional information on STP and MST on the Cisco 7600 series routers, see Configuring STP and MST at:


Overview of MST on EVC Bridge Domain

The MST on EVC Bridge-Domain feature uses VLAN IDs for service-instance-to-MST-instance mapping. EVC service instances with the same VLAN ID (the outer VLAN IDs in the QinQ case) as the one in another MST instance will be mapped to that MST instance.

EVC service instances can have encapsulations with a single tag as well as double tags. In case of double tag encapsulations, the outer VLAN ID shall be used for the MST instance mapping, and the inner VLAN ID is ignored.

A single VLAN per EVC is needed for the mapping with the MST instance. The following service instances without any VLAN ID or with multiple outer VLAN IDs are not supported:

- Untagged (encapsulation untagged)
- Priority-tagged (encapsulation priority-tagged)
- Default (encapsulation default)
- Multiple outer tags (encapsulation dot1q 200 to 400 second-dot1q 300)
Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines while configuring MST on EVC bridge domain:

- Cisco IOS Release 15.1(1)S supports EVC port-channels.
- Main interface where the EFP is configured must be up and running with MSTP as the selected Spanning Tree Mode (PVST and Rapid-PVST are not supported).
- The SPT PortFast feature is not supported with EFPs.
- The co-existence of REP and mLACP with MST on the same port is not supported.
- Any action performed on VPORT (which represents a particular VLAN in a physical port) affects the bridge domain and other services.
- This feature cannot co-exist with Ethernet Bridging on FR/ATM that support only PVST.
- Supports 64 MSTs and one CIST (common and internal spanning tree).
- Supports one MST region.
- Scales to 32000 EFP.
- Service instances without any VLAN ID in the encapsulation are not supported, because a unique VLAN ID is required to map an EVC to an MST instance.
- Supports EFPs with unambiguous outer VLAN tag (that is, no range, list on outer VLAN, neither default nor untagged).
- ES20 and ES+ line cards support this feature.
- Removing dot1q encapsulation removes the EVC from MST.
- Changing the VLAN (outer encapsulation VLAN of EVC) mapping to a different MST instance will move the EVC port to the new MST instance.
- Changing an EVC service instance to a VLAN that has not been defined in MST 1 will result in mapping of EVC port to MST 0.
- The peer router of the EVC port must also be running MST.
- MST is supported only on EVC BD. EVCs without BD configuration will not participate in MST.
- When an MST is configured on the outer VLAN, you can configure any number of service instances with the same outer VLAN as shown in the following configuration example.

```
nPE1#sh run int gi12/5
Building configuration...

Current configuration : 373 bytes
!
interface GigabitEthernet12/5
  description connected to CE1
  no ip address
  service instance 100 ethernet
    encapsulation dot1q 100 second-dot1q 1
    bridge-domain 100
  
  service instance 101 ethernet
    encapsulation dot1q 100 second-dot1q 2
    bridge-domain 101
  
  service instance 102 ethernet
    encapsulation dot1q 100 second-dot1q 120-140
    bridge-domain 102
```

Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide 4-85
Chapter 4  Configuring Layer 1 and Layer 2 Features

Configuring MST on EVC Bridge Domain

nPE1#sh run int gi12/6
Building configuration...

Current configuration : 373 bytes
!
interface GigabitEthernet12/6
description connected to CE1
no ip address
service instance 100 ethernet
  encapsulation dot1q 100 second-dot1q 1
  bridge-domain 100
!
service instance 101 ethernet
  encapsulation dot1q 100 second-dot1q 2
  bridge-domain 101
!
service instance 102 ethernet
  encapsulation dot1q 100 second-dot1q 120-140
  bridge-domain 102
!
end
end

nPE1# sh span vlan 100

MST0
  Spanning tree enabled protocol mstp
  Root ID  Priority   32768
    Address  0018.742f.3b80
    Cost     0
    Port     2821 (GigabitEthernet12/5)
    Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority   32768 (priority 32768 sys-id-ext 0)
    Address  001a.303c.3400
    Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Interface        Role Sts   Cost  Prio.Mbr  Type
  ----------------------- --- ------ ------ ------------
  Gi12/5           Root FWD 20000     128.2821 P2p
  Gi12/6           Altn BLK 20000     128.2822 P2p

nPE1#

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/port or interface tengigabitethernet slot/port
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id
6. [no] bridge-domain bridge-id
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable  | Enables privileged EXEC mode.  
       |         | • Enter your password if prompted. |
| 2    | configure terminal | Enters global configuration mode. |
| 3    | interface gigabitethernet slot/port  
      | or  
      | interface tengigabitethernet slot/port | Specifies the gigabit ethernet or the ten gigabit ethernet interface to configure.  
      |         | • slot/port—Specifies the location of the interface. |
|      | service instance id Ethernet  
      | [service-name] | Creates a service instance (EVC instance) on an interface and sets the device into the config-if-srv submode. |
| 4    | encapsulation dot1q vlan-id | Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance. |
| 5    | bridge-domain bridge-id | Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance. |

### Examples

In the following example, two interfaces participate in MST instance 0, the default instance to which all VLANs are mapped:

```
Router# enable
Router# configure terminal
Router(config)# interface g4/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 2
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# interface g4/3
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 2
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# end
```
Verification

Use this command to verify the configuration:

Router# show spanning-tree vlan 2

MST0
Spanning tree enabled protocol mstp
Root ID Priority 32768
Address 0009.e91a.bc40
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0009.e91a.bc40
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi4/1 Desg FWD 20000 128.1537 P2p
Gi4/3 Back BLK 20000 128.1540 P2p

In this example, interface gi4/1 and interface gi4/3 are connected back-to-back. Each has a service
instance (EFP) attached to it. The EFP on both interfaces has an encapsulation VLAN ID of 2. Changing
the VLAN ID from 2 to 8 in the encapsulation directive for the EFP on interface gi4/1 stops the MSTP
from running in the MST instance to which the old VLAN is mapped and starts the MSTP in the MST
instance to which the new VLAN is mapped:

Router(config-if)# interface gi4/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encap dot1q 8
Router(config-if-srv)# end

Use this command to verify the configuration:

Router# show spanning-tree vlan 2

MST1
Spanning tree enabled protocol mstp
Root ID Priority 32769
Address 0009.e91a.bc40
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0009.e91a.bc40
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi4/3 Desg FWD 20000 128.1540 P2p

Router# show spanning-tree vlan 8

MST2
Spanning tree enabled protocol mstp
Root ID Priority 32770
Address 0009.e91a.bc40
This bridge is the root
Configuring MST on EVC Bridge Domain

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 0009.e91a.bc40
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi4/1 Desg FWD 20000 128.1537 P2p

In this example, interface gi4/3 (with an EFP that has an outer encapsulation VLAN ID of 2 and a bridge domain of 100) receives a new service:

Router# enable
Router# configure terminal
Router(config)# interface g4/3
Router((config-if)# service instance 2 ethernet
Router((config-if-srv)# encaps dot1q 2 second-dot1q 100
Router((config-if-srv)# bridge-domain 200

Now there are two EFPs configured on interface gi4/3 and both of them have the same outer VLAN 2.

interface GigabitEthernet4/3
  no ip address
  service instance 1 ethernet
  encapsulation dot1q 2
  bridge-domain 100
  !
  service instance 2 ethernet
  encapsulation dot1q 2 second-dot1q 100
  bridge-domain 200

The preceding configuration does not affect the MSTP operation on the interface; there is no state change for interface gi4/3 in the MST instance it belongs to.

Router# show spanning-tree mst 1

### MST1 vlans mapped: 2
Bridge address 0009.e91a.bc40 priority 32769 (32768 sysid 1)
Root this switch for MST1

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi4/3 Desg FWD 20000 128.1540 P2p

This example shows MST on port channels:

Router# show spanning-tree mst 1

### MST1 vlans mapped: 3
Bridge address 000a.f331.8e80 priority 32769 (32768 sysid 1)
Root address 0001.6441.68c0 priority 32769 (32768 sysid 1)
port Po5 cost 20000 rem hops 18

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
G12/0/0 Desg FWD 20000 128.257 P2p
Po5 Root FWD 10000 128.3329 P2p
Po6 Altn BLK 10000 128.3330 P2p

Router# show spanning-tree vlan 3

MST1
Spanning tree enabled protocol mstp
Root ID Priority 32769
Address 0001.6441.68c0
Cost 20000
Port 3329 (Port-channel5)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000a.f331.8e80
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/0/0</td>
<td>Desg</td>
<td>FWD</td>
<td>20000</td>
<td>128.257</td>
<td>P2p</td>
</tr>
<tr>
<td>Po5</td>
<td>Root</td>
<td>FWD</td>
<td>10000</td>
<td>128.3329</td>
<td>P2p</td>
</tr>
<tr>
<td>Po6</td>
<td>Altn</td>
<td>BLK</td>
<td>10000</td>
<td>128.3330</td>
<td>P2p</td>
</tr>
</tbody>
</table>

Troubleshooting

Table 4-15 provides troubleshooting solutions for the MST on EVC Bridge Domain feature.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Spanning Tree Protocol (MSTP) incorrectly or inconsistently</td>
<td>To avoid BPDU loss, re-configure these on the following nodes:</td>
</tr>
<tr>
<td>formed due to misconfiguration and BPDU loss</td>
<td>• Configuration name</td>
</tr>
<tr>
<td></td>
<td>• Bridge revision</td>
</tr>
<tr>
<td></td>
<td>• Provider-bridge mode</td>
</tr>
<tr>
<td></td>
<td>• Instance to VLAN mapping</td>
</tr>
<tr>
<td></td>
<td>Determine if node A is sending BPDUs to node B. Use the show</td>
</tr>
<tr>
<td></td>
<td>spanning-tree mst interface gi1/1 service instance command for each</td>
</tr>
<tr>
<td></td>
<td>interface connecting the nodes. Only designated ports relay periodic</td>
</tr>
<tr>
<td></td>
<td>BPDPUs. Use the debug spanning-tree mst packet full {received</td>
</tr>
<tr>
<td></td>
<td>to debug topology change notifications. Use the debug spanning-tree mst</td>
</tr>
<tr>
<td></td>
<td>packet brief {received</td>
</tr>
<tr>
<td></td>
<td>the timestamps. A time gap greater than or equal to six seconds causes</td>
</tr>
<tr>
<td></td>
<td>topology change.</td>
</tr>
<tr>
<td>MSTP correctly formed, but traffic flooding occurs</td>
<td>Intermittent BPDU loss occurs when the spanning tree appears incorrectly</td>
</tr>
<tr>
<td></td>
<td>in the show commands, but relays topology change notifications. These</td>
</tr>
<tr>
<td></td>
<td>notifications cause a MAC flush, forcing traffic to flood until the MAC</td>
</tr>
<tr>
<td></td>
<td>addresses are re-learned. Use the debug spanning-tree mst packet full</td>
</tr>
<tr>
<td></td>
<td>{received</td>
</tr>
<tr>
<td></td>
<td>spanning-tree mst packet brief {received</td>
</tr>
<tr>
<td></td>
<td>to check for missing BPDPUs. Monitor the timestamps. A time gap greater</td>
</tr>
<tr>
<td></td>
<td>than or equal to six seconds causes topology change.</td>
</tr>
</tbody>
</table>
### Configuring Link State Tracking (LST)

When a link failure occurs on a REP and MST segment, the associated protocols handle the link failure event. However, if the primary link to the switch is enabled even though the corresponding uplink ports on the switch are disabled, the REP and MST protocol is unaware of backbone side, and does not trigger a failover. The router continues to receive the traffic from the access side and then drops it discreetly due to lack of backbone connectivity. Link state tracking provides a solution to this problem by allowing the uplink interfaces to bind the link status to the down link ports. Uplink state tracking is configured such that when a set of uplink ports are disabled, other ports linked through CLI commands are disabled as well. The state of all the downlink interfaces are error-disabled only when all the upstream interfaces are disabled.

The LST triggers REP/MST re-convergence on the access side depending on the state of the core-facing interface. The link state of the core facing interface and the access facing interface are bound by link state tracking group.

LST facilitates:
- Enabling and disabling of link state group tracking.
- Removal of downstream interfaces from a link state group.
- Performing shut/no shut on error disabled interface.

### Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines when you configure the LST:

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSTP shows incorrect port state</td>
<td>When the spanning tree protocol (STP) attempts to change the port state, it uses L2VPN. Check the value of the sent update. If the value is Yes, then STP is awaiting an update from L2VPN.</td>
</tr>
</tbody>
</table>
| Packet forwarding does not match the MSTP state | Complete the following steps to verify and troubleshoot:  
  1. Shut down redundant links, remove MSTP configuration, and ensure that basic bridging works.  
  2. Check the state of each port as calculated by MSTP, and compare it with the packet counts transmitted and received on ports and EFPs controlled by MSTP. Normal data packets should be sent/received only on ports in the forwarding (FWD) state. BPDUs should be sent/received on all ports controlled by MSTP.  
  3. Ensure that BPDUs are flowing and that root bridge selection is correct and check the related scenarios.  
  4. Use the `show l2vpn bridge-domain detail` command to confirm the status of the members of the bridge domain. Ensure that the relevant bridge domain members are active.  
  5. Check the forwarding state as programmed in hardware. |
- Ensure that the management interfaces are not part of a link state group.
- REP port cannot be configured as uplink port.
- LST does not allow any interface, upstream or downstream, to be part of more than one link state group.
- You can configure a maximum of 10 link state groups.
- When you configure LST for the first time, you must add upstream interfaces to the link state group before adding downstream, otherwise the state of the downlink interfaces are error-disabled.
- The configurable interfaces are physical (both routed and switch port), port-channel, sub-interface and VLAN.
- Upstream interfaces are required to be among:
  - L3 interface (physical or portchannel)
  - SVI
- Downstream interfaces are required to be among:
  - L2 interface
  - L2 Port-channel
  - EVC

## Configuring Link State Tracking

Perform the following tasks to configure a LST.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `link state track number`
4. `interface slot/port`
5. `link state group [number] /upstream | downstream`
6. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 3**

```
link state track number
```

Example:
```
Router(config)# link state track 1
```

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a link-state group and enables LST. The acceptable range is 1-10; the default value is 1.</td>
</tr>
</tbody>
</table>

**Step 4**

```
interface slot/port
```

Example:
```
Router(config)# interface gigabitethernet 2/1
```

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures an interface.</td>
</tr>
</tbody>
</table>

**Step 5**

```
link state group [number] {upstream | downstream}
```

Example:
```
Router(config-if)# link state group 1 upstream
```

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies a link-state group and configures the interface as either an upstream or downstream interface in the group. The group number can be 1 to 10; the default value is 1.</td>
</tr>
</tbody>
</table>

**Step 6**

```
end
```

Example:
```
Router(config-if)# end
```

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exits the CLI to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

This example shows how to create a link-state group and configure the interfaces:

```
Router# configure terminal
Router(config)# link state track 1
Router(config)# interface gigabitethernet3/1
Router(config-if)# link state group 1 upstream
Router(config-if)# interface gigabitethernet3/3
Router(config-if)# link state group 1 upstream
Router(config-if)# interface gigabitethernet3/5
Router(config-if)# link state group 1 downstream
Router(config-if)# interface gigabitethernet3/7
Router(config-if)# link state group 1 downstream
Router(config-if)# end
```

### Verification

Use the `show link state group` command to display the link-state group information.
```
Router> show link state group 1
Link State Group: 1 Status: Enabled, Down
```

Use the `show link state group detail` command to display detailed information about the group.
```
Router> show link state group detail
(Up): Interface up (Dwn): Interface Down (Dis): Interface disabled
Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi3/5(Dwn) Gi3/6(Dwn)
Downstream Interfaces : Gi3/1(Dis) Gi3/2(Dis) Gi3/3(Dis) Gi3/4(Dis)
Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi3/15(Dwn) Gi3/16(Dwn) Gi3/17(Dwn)
Downstream Interfaces : Gi3/11(Dis) Gi3/12(Dis) Gi3/13(Dis) Gi3/14(Dis)
(Up): Interface up (Dwn): Interface Down (Dis): Interface disabled
Troubleshooting the Link State Tracking

Table 4-16 lists the troubleshooting issues while configuring LST:

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The downstream interface is in error-disabled state even though the upstream interfaces are up.</td>
<td>Use the <code>show interfaces &lt;interface&gt; status err-disabled</code> command to check why the interface is in such state. Use the <code>show errdisable recovery</code> command to view information about the error-disable recovery timer.</td>
</tr>
</tbody>
</table>

MAC Address Security for EVC Bridge Domain

Cisco 7600 series routers currently support port security on a per-port basis. For more information, see Configuring Port Security at:


The Media Access Control (MAC) Address Security for EVC Bridge Domain feature addresses port security with EVCs by providing the capability to control and filter MAC address learning behavior at the granularity of a per-EFP basis. For instance, when a violation requires a shutdown, only the customer assigned to a given EFP is affected rather than all customers using the port.

Port Security and the MAC Address Security for EVC Bridge Domain feature operate independently of each other.

Cisco IOS Release 12.2(33)SRE adds support for MAC address security on EVC port-channels. This feature operates on a port-channel interface in a similar manner to how it works on a physical port. In each case, MAC security is configured on a service instance associated with a bridge domain.

This section covers the following topics: This section contains the following topics:

- Restrictions and Usage Guidelines, page 4-95
- Enabling MAC Address Security for EVC Bridge Domain, page 4-95
- Enabling MAC Address Security for EVC Bridge Domain, page 4-95
- Disabling MAC Address Security for EVC Bridge Domain on an EFP, page 4-97
- Configuring MAC Address Whitelist on an EFP, page 4-98
- Configuring Sticky MAC Addresses on an EFP, page 4-100
- Configuring Secure MAC Address Aging on an EFP, page 4-102
- Configuring MAC Address Limiting on EFP, page 4-105
- Configuring MAC Address Limiting on a Bridge Domain, page 4-106
- Configuring Violation Response on an EFP, page 4-107
Restrictions and Usage Guidelines

When configuring MAC Address Security for EVC Bridge Domain, follow these restrictions and usage guidelines:

- System wide, the following limits apply to the total configured whitelist and learned MAC addresses:
  - Total number of MAC addresses supported under MAC Security is limited to 32K.
  - Total number of MAC addresses supported under MAC Security, per bridge domain, is limited to 10K.
  - Total number of MAC addresses supported under MAC Security, per EFP, is limited to 1K.

- You can configure or remove the various MAC security elements irrespective of whether MAC security is enabled on the EFP. However, these configurations will become operational only after MAC security is enabled.

- Upon enabling the MAC Address Security for EVC Bridge Domain feature, existing MAC address table entries on the EFP are removed.

- The MAC Address Security for EVC Bridge Domain feature can be configured on an EFP only if the EFP is a member of a bridge domain.

- If you disassociate the EFP from the BD, the MAC security feature is completely removed.

- For port-channel, this configuration is propagated to all member links in the port-channel. Consistent with the already implemented bridge domain EVC port-channel functionality, packets on a secured EFP are received on any member link, but all the egress packets are sent out to one of the selected member links.

- MAC security is not supported on MTP and C-MAC bridge domain.

Enabling MAC Address Security for EVC Bridge Domain

This section describes how to enable MAC address security for EVC bridge domain.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id
6. bridge-domain bridge-id
7. mac security
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enable privileged EXEC mode.</td>
</tr>
<tr>
<td>Enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Example:</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.</td>
</tr>
<tr>
<td>interface gigabitethernet slot/subslot/port</td>
<td>Example:</td>
</tr>
<tr>
<td>or interface tengigabitethernet slot/subslot/port</td>
<td>Example:</td>
</tr>
<tr>
<td>or interface port-channel number</td>
<td>Router(config)# interface gigabitethernet 4/1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td>service instance id Ethernet [service-name]</td>
<td>Example:</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# service instance 101 ethernet</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td>encapsulation dot1q vlan-id</td>
<td>Example:</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-srv)# encapsulation dot1q 13</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.</td>
</tr>
<tr>
<td>bridge-domain bridge-id</td>
<td>Example:</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-srv)# bridge-domain 12</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Enables or disables the MAC Security on the EFP.</td>
</tr>
<tr>
<td>mac security or no mac security</td>
<td>Example:</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-srv)# mac security or Router(config-if-srv)# no mac security</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to enable MAC address security for EVC bridge domain.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1
```
MAC Address Security for EVC Bridge Domain

This example shows how to disable MAC address security for EVC bridge domain.

Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 4/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# mac security

Disabling MAC Address Security for EVC Bridge Domain on an EFP

This section describes how to disable MAC address security for EVC bridge domain.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. no mac security

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number</td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MAC Address Security for EVC Bridge Domain

### Examples

This example shows how to disable MAC address security for EVC bridge domain.

```plaintext
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# service instance 101 ethernet
```

### Configuring MAC Address Whitelist on an EFP

MAC addresses learned dynamically on the EFP after mac security sticky is configured are retained during a link-down condition and device reload. Sticky Mac is shown in the MAC table as static addresses. However, you should copy the running config details to retain the mac address details.

This section describes how to configure sticky MAC addresses on an EFP.

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id
6. bridge-domain bridge-id
7. mac security sticky
8. mac security
9. no mac security
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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/subslot/port
  or
  * interface tengigabitethernet slot/subslot/port
  or
  * interface port-channel number
  **Example:**
  
  ```
  Router(config)# interface gigabitethernet 4/1
  ```
  
  Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure. |
| **Step 4**
  * service instance id Ethernet [service-name]
  **Example:**
  
  ```
  Router(config-if)# service instance 101 ethernet
  ```
  
  Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode. |
| **Step 5**
  * encapsulation dot1q vlan-id
  **Example:**
  
  ```
  Router(config-if-srv)# encapsulation dot1q 13
  ```
  
  Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance. |
| **Step 6**
  * bridge-domain bridge-id
  **Example:**
  
  ```
  Router(config-if-srv)# bridge-domain 12
  ```
  
  Binds the service instance to a bridge domain instance where `bridge-id` is the identifier for the bridge domain instance. |
| **Step 7**
  * mac security address permit mac address
  **Example:**
  
  ```
  Router(config-if-srv)# mac security address permit 0000.1111.2222
  ```
  
  Adds the specified MAC Address as a whitelist ("permit") MAC Address for the EFP. |
| **Step 8**
  * mac security
  **Example:**
  
  ```
  Router(config-if-srv)# mac security
  ```
  
  Enables MAC Security on the EFP. |
Examples

This example shows how to configure whitelisted MAC addresses on an EFP that is a member of a bridge domain.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# service instance 10 ethernet
Router(config-srv)# encapsulation dot1q 20
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security address permit 0000.1111.2222
Router(config-if-srv)# mac security
```

Configuring Sticky MAC Addresses on an EFP

MAC addresses learned dynamically on the EFP after mac security sticky is configured are retained during a link-down condition and device reload. Sticky Mac is shown in the MAC table as static addresses. However, you should copy the running config details to retain the mac address details.

This section describes how to configure sticky MAC addresses on an EFP.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id
6. bridge-domain bridge-id
7. mac security sticky
8. mac security
9. no mac security

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Command Purpose

| Step 3 | **interface gigabitethernet**<br>slot/sublot/port<br>or<br>**interface tengigabitethernet**<br>slot/sublot/port<br>or<br>**interface port-channel** number<br>  
Example:<br>Router(config)# interface gigabitethernet 4/1 | Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure. |
| Step 4 | **service instance** id Ethernet<br> [service-name]  
Example:<br>Router(config-if)# service instance 101 ethernet | Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode. |
| Step 5 | **encapsulation dot1q** vlan-id  
Example:<br>Router(config-if-srv)# encapsulation dot1q 13 | Defines the matching criteria to be used in order to map ingress dot1q frames (double tagged) on an interface to the appropriate service instance. |
| Step 6 | **bridge-domain** bridge-id  
Example:<br>Router(config-if-srv)# bridge-domain 12 | Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance. |
| Step 7 | **mac security sticky**  
Example:<br>Router(config-if-srv)# mac security sticky | Enables Sticky feature causing all dynamic secure MAC addresses to become sticky MAC addresses. Any new MAC address learnt becomes sticky.  
**Note** To retain the sticky MAC addresses across reloads, ensure that you save the running configuration to the start up configuration. |
| Step 8 | **mac security**  
Example:<br>Router(config-if-srv)# mac security | Enables MAC Security on the EFP. |
| Step 9 | **no mac security**  
Example:<br>Router(config-if-srv)# no mac security | Disables the MAC Security on the EFP. |

### Examples

This example configures sticky MAC addresses on an EFP.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 20
```
MAC Address Security for EVC Bridge Domain

Configuring Secure MAC Address Aging on an EFP

This section shows how to configure aging of secured MAC addresses under MAC Security. Secured MAC addresses are not subject to the normal aging of MAC table entries in the system. By default, secure MAC addresses do not age out.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id double tagged
6. bridge-domain bridge-id
7. mac security aging time m [inactivity]
8. mac security aging static
9. mac security aging sticky
10. mac security
11. no mac security

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 4 Configuring Layer 1 and Layer 2 Features

## MAC Address Security for EVC Bridge Domain

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>interface gigabitethernet &lt;slot/subslot/port&gt; or interface tengigabitethernet &lt;slot/subslot/port&gt; or interface port-channel &lt;number&gt;</td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.</td>
</tr>
<tr>
<td>4</td>
<td>service instance &lt;id&gt; Ethernet [service-name]</td>
<td>Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td>5</td>
<td>encapsulation dot1q &lt;vlan-id&gt;</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q double-tagged frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td>6</td>
<td>bridge-domain &lt;bridge-id&gt;</td>
<td>Binds the service instance to a bridge domain instance where &lt;bridge-id&gt; is the identifier for the bridge domain instance.</td>
</tr>
<tr>
<td>7</td>
<td>mac security aging time &lt;m&gt; [inactivity]</td>
<td>Sets the aging time for secure addresses (range is 0-1440). The optional inactivity keyword specifies that the address aging is due to inactivity of the sending hosts (as opposed to absolute aging).</td>
</tr>
<tr>
<td>8</td>
<td>mac security aging static</td>
<td>Applies aging controls to statically configured addresses.</td>
</tr>
<tr>
<td>9</td>
<td>mac security aging sticky</td>
<td>Applies aging controls to sticky addresses.</td>
</tr>
</tbody>
</table>
MAC Address Security for EVC Bridge Domain

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 10</td>
<td>mac security</td>
</tr>
<tr>
<td>Example:</td>
<td>Enables MAC Security on the EFP. A sticky MAC address on the MAC table is shown as static addresses.</td>
</tr>
<tr>
<td>Step 11</td>
<td>no mac security</td>
</tr>
<tr>
<td>Example:</td>
<td>Disables the MAC Security on the EFP.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure the aging time for secure addresses to 10 minutes.

Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 20
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security aging time 10

This example shows a configuration where the aging out of addresses is based on inactivity of the sending hosts. An address will age out if it is not seen for 10 minutes.

Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 20
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security aging time 10 inactivity

The **mac security aging time** command only ages out secure addresses that are learned. To enable aging out of whitelist or sticky addresses when the **mac security aging time** command is configured, use the **mac security aging static** command (applies aging controls to statically configured addresses) or the **mac security aging sticky** command (applies aging controls to persistent, that is, sticky, addresses). The configuration below shows an example of applying aging to a sticky address.

Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 1/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security
Router(config-if-srv)# mac security sticky
Router(config-if-srv)# mac security aging time 100

**Step 10: mac security**

Example:

```
Router(config-if-srv)# mac security
```

Enables MAC Security on the EFP. A sticky MAC address on the MAC table is shown as static addressess.

**Step 11: no mac security**

Example:

```
Router(config-if-srv)# no mac security
```

Disables the MAC Security on the EFP.
Configuring MAC Address Limiting on EFP

This section describes how to configure an upper limit for the number of secured MAC addresses allowed on an EFP. This includes addresses added as part of a whitelist, as well as dynamically learned MAC addresses. If the upper limit is decreased, one or more learned MAC entries may be removed. The default limit is 1.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id double tagged
6. bridge-domain bridge-id
7. mac security maximum addresses n
8. mac security

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router# enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number</td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.</td>
</tr>
<tr>
<td>Example: Router(config)# interface gigabitethernet 4/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id Ethernet [service-name]</td>
<td>Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td>Example: Router(config-if)# service instance 101 ethernet</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring MAC Address Security for EVC Bridge Domain

**Examples**

This example configures an upper limit of 10 for the number of secured MAC addresses allowed on an EFP.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 20
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security maximum addresses 10
```

### Configuring MAC Address Limiting on a Bridge Domain

This section describes how to configure an upper limit for the number of secured MAC addresses located on the bridge domain.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **bridge-domain** `vlan-id [access | dot1q [tag] | dot1q-tunnel] [broadcast] [ignore-bpdu-pid] [pvst-tlv CE-vlan] [increment] [lan-fcs] [split-horizon]`
4. **mac limit maximum addresses [n]**
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Router# enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>bridge-domain vlan-id [access</td>
<td>dot1q [tag]</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config)# bridge-domain 12</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>mac limit maximum addresses [n]</td>
<td>Sets the limit for maximum addresses. The default value is 10240.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-bdomain)# mac limit maximum addresses 1000</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

This example configures an upper limit of 1000 for the number of secured MAC addresses.

```
Router# enable
Router# configure terminal
Router(config)# bridge-domain 100
Router(config-if-srv)# mac limit maximum address 1000
```

### Configuring Violation Response on an EFP

This section describes how to specify the expected behavior of the device when an attempt to dynamically learn a MAC address fails because of a violation of the configured MAC Security policy on the EFP. The default violation behavior is termed as a EFP shutdown.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id
6. bridge-domain bridge-id
7. `mac security violation restrict` or `mac security violation protect`

8. `mac security`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt;Enable privileged EXEC mode.&lt;br&gt;Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>Router# enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>interface gigabitethernet slot/subslot/port</strong>&lt;br&gt;or&lt;br&gt;<strong>interface tengigabitethernet slot/subslot/port</strong>&lt;br&gt;or&lt;br&gt;<strong>interface port-channel number</strong>&lt;br&gt;Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config)# interface gigabitethernet 4/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>service instance id Ethernet [service-name]</strong>&lt;br&gt;Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config-if)# service instance 101 ethernet</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>encapsulation dot1q vlan-id</strong>&lt;br&gt;Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config-if-srv)# encapsulation dot1q 13</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>bridge-domain bridge-id</strong>&lt;br&gt;Binds the service instance to a bridge domain instance where <code>bridge-id</code> is the identifier for the bridge domain instance.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config-if-srv)# bridge-domain 12</code></td>
<td></td>
</tr>
</tbody>
</table>
Step 7  mac security violation restrict  
or  
    or  
mac security violation protect  

Example:  
Router(config-if-srv)# mac security violation restrict  

Sets the violation mode to restrict or protect.  
The no version of this command sets the violation  
response back to default (default is shutdown). In the  
Restrict scenario, the packets are dropped and an error  
message is displayed about the log warning level; in the  
Protect scenario, the packets are silently dropped and  
no messages are displayed.

Step 8  mac security  

Example:  
Router(config-if-srv)# mac security  

Enables MAC Security on the EFP.

Examples

This example configures a restrict violation response on EFP.

Router# enable  
Router# configure terminal  
Router(config)# interface GigabitEthernet 2/1  
Router(config-if)# service instance 10 ethernet  
Router(config-if)# encapsulation dot1q 20  
Router(config-if)# bridge-domain 100  
Router(config-if)# mac security violation restrict  
Router(config-if-srv)# mac security

Error Recovery

This section describes how to recover from violation causing an EFP shutdown (default violation  
response) and contains the following sections:

Manual recovery  
Automatic recovery

Manual Recovery

For manual recovery, use the clear ethernet service instance id id interface interface-name errdisable  
command to bring the service instance out of an error disabled state as shown below:

Router# enable  
Router# configure terminal  
Router# clear ethernet service instance id 10 interface gi1/1 errdisable

Automatic recovery

For automatic recovery, use the errdisable recovery cause mac security command. You must specify  
the timer interval. The valid value is from 30 to 86400 second. In the configuration example that follows,  
the EFP recovers 60 seconds after the violation causes the shutdown.

Router# enable  
Router# configure terminal

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 7 mac security violation restrict  
or  
mac security violation protect  | Sets the violation mode to restrict or protect.  
The no version of this command sets the violation response back to default (default is shutdown). In the Restrict scenario, the packets are dropped and an error message is displayed about the log warning level; in the Protect scenario, the packets are silently dropped and no messages are displayed. |
| Step 8 mac security  | Enables MAC Security on the EFP. |
MAC Address Security for EVC Bridge Domain

```
Router(config)# interface GigabitEthernet 2/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security
Router(config-if-srv)# errdisable recovery cause mac-security 60
```

Verification

Use the following commands to verify operation.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ethernet service instance id id interface mac security address</td>
<td>Displays the secure addresses on the specified EFP.</td>
</tr>
<tr>
<td>Router# show ethernet service instance id id interface mac security last violation</td>
<td>Displays the last violation recorded on the specified EFP.</td>
</tr>
<tr>
<td>Router# show ethernet service instance id id interface mac security statistics</td>
<td>Displays the number of allowed and actual secured address and the number of violations recorded on the EFP.</td>
</tr>
<tr>
<td>Router# show ethernet service instance id id interface mac security</td>
<td>Displays the MAC Security status of the specified EFP.</td>
</tr>
<tr>
<td>Router# show ethernet service instance mac security address</td>
<td>Displays the secure addresses on all the EFPs in the system.</td>
</tr>
<tr>
<td>Router# show ethernet service instance mac security last violation</td>
<td>Displays information about the last violation recorded on the device (across all service instances) and information about the last violation recorded on each of the service instances.</td>
</tr>
<tr>
<td>Router# show ethernet service instance mac security statistics</td>
<td>Displays the number of allowed and actual secured addresses, as well as the number of violations recorded on all the EFPs in the system.</td>
</tr>
<tr>
<td>Router# show ethernet service instance mac security</td>
<td>Displays all the EFPs in the system that have MAC Security enabled.</td>
</tr>
<tr>
<td>Router# show bridge-domain id mac security address</td>
<td>Displays the secure addresses on all EFPs belonging to the specified bridge domain.</td>
</tr>
<tr>
<td>Router# show bridge-domain id mac security last violation</td>
<td>Displays information about the last violation recorded on each of the service instances belonging to the bridge domain.</td>
</tr>
<tr>
<td>Router# show bridge-domain id mac security statistics</td>
<td>Displays the number of allowed and actual secured addresses, as well as the number of violations recorded on all the EFPs that belong to the specified bridge domain.</td>
</tr>
<tr>
<td>Router# show bridge-domain id mac security</td>
<td>Displays all the EFPs that belong to the specified bridge domain, and that have MAC Security enabled.</td>
</tr>
</tbody>
</table>

Troubleshooting

Table 4-17 provides troubleshooting solutions for the MAC Security feature.
Table 4-17  Troubleshooting Scenarios for MAC Security feature

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC security errors on the RP</td>
<td>Use the <code>debug ethernet service instance id id interface int mac sec errors</code> and <code>debug ethernet service instance id id interface int mac table errors</code> commands. Share the output with TAC for further investigation.</td>
</tr>
<tr>
<td>MAC security errors on the SP</td>
<td>Use the <code>debug ethernet service instance mac security errors</code> and <code>debug ethernet service instance mac table errors</code> commands to troubleshoot mac security issues on the RP.</td>
</tr>
<tr>
<td>EFP is disabled and is unable to automatically recover from error disable state</td>
<td>Use the <code>errdisable recovery cause mac-security interval or clear ethernet service instance id id interface interface-name errdisable</code> commands to re-enable the EFP.</td>
</tr>
<tr>
<td>Mac security aging timer is inactive</td>
<td>When <code>mac security aging time inactivity</code> is configured, the hardware mac table aging timer for the EFP VLAN is set with the configuration command <code>mac address-table aging-time time [vlan &lt;vlan id&gt;]</code> command. To resolve the aging timer inactivity, re-set the aging time to the default value of 300 seconds.</td>
</tr>
</tbody>
</table>

CFM and PVST Co-Existence

Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance Ethernet layer OAM protocol that includes proactive connectivity monitoring, fault verification, and fault isolation. Currently, Ethernet CFM supports inward facing and outward facing Maintenance Endpoints (MEPs). For information on Ethernet Connectivity Fault Management, see [http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srethcfm.html](http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srethcfm.html).

The CFM and PVST Co-Existence feature allows Per Vlan Spanning Tree (PVST) and CFM to co-exist on Cisco 7600 series routers.

The CFM and PVST Co-Existence feature makes use of these Ethernet components:

- Ethernet virtual circuit (EVC)—An association between two or more UNIs that identifies a point-to-point or point-to-multipoint path within the provider network.
- Ethernet flow point (EFP)—The logical demarcation point of an EVC on an interface.

Each EFP is identified with an EVC. An EVC ID is globally unique within a network. In addition, an EFP is associated with one bridge domain. All the EFPs in a bridge domain belong to the same EVC (when specified).

For EFPs, untagged, single-tagged, and double-tagged encapsulations exist with dot1q, QinQ, and IEEE dot1ad Ether types. Different EFPs belonging to a bridge domain can have different encapsulations.

Restrictions and Usage Guidelines

When configuring CFM and PVST Co-Existence, follow these restrictions and usage guidelines:

- The following line cards and supervisors that have three or more match registers are supported:
  - ES20 line cards
- ES+ line cards
- RSP720-3C-10GE and
- Supervisor Engine 32
- WS-X67xx line cards (with supported supervisor)

- Generic VLAN Registration Protocol (GVRP) and CFM coexistence is also supported

- The following co-existing configurations are supported:
  - PVST and CFM; you must configure PVST before configuring CFM
  - Generic VLAN Registration Protocol (GVRP) and CFM; you must configure GVRP before configuring CFM
  - PVST and GVRP; there is no restriction for the order of configuration.

- CFM uses two match registers to identify the control packet type; PVST also uses a match register to identify its control packet type. So in order for both protocols to work on the same system each line card needs to support three match registers, at least one being able to support only a 44 bit MAC match.

  - This message is displayed when no match registers are available.

CFM is enabled system wide except on supervisor ports due to spanning tree configuration on supervisor ports for CFM due to hardware limitations on these ports. Continued with enabling CFM system-wide to allow coexistence with other protocols such as PVST.

Administrator action may be required. Ensure no CFM traffic is presented to any supervisor ports via configuration. If not possible configure STP mode to MST and re-enable CFM or disable CFM completely.

  - This message is displayed when the 48 bit match register is not available.

CFM is enabled system wide except it’s disabled on supervisor ports due to spanning tree or GVRP configuration. Unable to program all port ASIC MAC match registers on supervisor ports for CFM due to hardware limitations on these ports. Continued with enabling CFM system-wide to allow coexistence with other protocols such as PVST or GVRP. System has handled this by disabling CFM on all supervisor ports. If this is unacceptable configure STP mode to MST and re-enable CFM or disable CFM completely.

  - This message is displayed, if after configuring PVST-CFM or GVRP-CFM co-existence, an attempt is made to power up an unsupported line card or to insert an unsupported line card into the router:

Unsupported module in slot 3, power not allowed: Module has insufficient match registers. Enabled relevant protocols include SSTP CFM_MULTICAST.

Note

Slot 3 in the above message refers to the module with insufficient match registers.
Configuring PVST and CFM Co-Existence

**Note**  
PVST mode is the default spanning-tree mode. It is enabled when you boot the router.

**Note**  
You cannot disable PVST spanning-tree mode or MST spanning-tree mode with the `no` versions of the `spanning-tree mode mst` or `spanning-tree mode pvst` commands; you must enable the other spanning-tree mode to disable the existing spanning-tree mode. For example, if you want to disable the MST spanning-tree mode, you must enable the PVST spanning-tree mode.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `spanning-tree mode pvst`
4. `ethernet cfm enable`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Router# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>spanning-tree mode pvst</code></td>
<td>Configures Per-VLAN Spanning Tree+ (PVST+) mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# <code>spanning-tree mode pvst</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>ethernet cfm enable</code></td>
<td>Enables connectivity fault management (CFM) processing globally on a device.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# <code>ethernet cfm enable</code></td>
<td></td>
</tr>
</tbody>
</table>

The following example configures PVST and CFM Co-Existence:

```
Router# enable
Router# configure terminal
Router(config)# spanning-tree mode pvst
Router(config)# ethernet cfm enable
```
Configuring GVRP and CFM Co-Existence

SUMMARY STEPS

1. enable
2. configure terminal
3. gvrp global
4. ethernet cfm enable

DETAIL STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> gvrp global</td>
<td>Enable GVRP globally.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# gvrp global</td>
<td>Enable GVRP globally.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ethernet cfm enable</td>
<td>Enables connectivity fault management (CFM) processing globally on a device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ethernet cfm enable</td>
<td>Enables connectivity fault management (CFM) processing globally on a device.</td>
</tr>
</tbody>
</table>

The following example configures GVRP and CFM Co-Existence:

Router# enable
Router# configure terminal
Router(config)# gvrp global
Router(config)# ethernet cfm enable

Configuring PVST and GVRP Co-Existence

SUMMARY STEPS

1. enable
2. configure terminal
3. gvrp global
4. spanning-tree mode pvst
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2  configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure</td>
<td></td>
</tr>
<tr>
<td>Step 3  gvrp</td>
<td>Enable GVRP globally.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# gvrp</td>
<td></td>
</tr>
<tr>
<td>Step 4  spanning-tree</td>
<td>Configures Per-VLAN Spanning Tree+ (PVST+) mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# spanning-tree</td>
<td></td>
</tr>
</tbody>
</table>

The following example configures PVST and GVRP Co-Existence:

```plaintext
Router# enable
Router# configure terminal
Router(config)# gvrp global
Router(config)# ethernet cfm enable
Router(config)# spanning-tree mode pvst
```

Verification

Use the following commands to verify operation.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show running configuration</td>
<td>Displays the contents of the current running configuration file or the configuration for a specific module.</td>
</tr>
<tr>
<td>Router# remote command switch show platform mrm info</td>
<td>Displays protocols using port ASIC match registers. However, the feature will not be enabled if the match registers are not programmed.</td>
</tr>
</tbody>
</table>

Custom Ethertype for EVC Interfaces

The custom ethertype feature allows you to configure the ethertype to be used for outer tag for dot1q and QinQ packets. By default, the Cisco 7600 series router supports ethertype 0x8100 for dot1q and QinQ outer tags. The following ethertype can be configured under a physical port:

- 0x8100 – 802.1q
- 0x9100 – Q-in-Q
Custom Ethertype for EVC Interfaces

- 0x9200 – Q-in-Q, and
- 0x88a8 – 802.1ad

You can use the `dot1q tunneling ethertype ethertype-value` command to configure the custom ethertype within a physical port.

In the following sample configuration, ethertype is set to 0x9100, service instance is created, and Rewrite process is initiated:

```
interface GigabitEthernet 1/1
  dot1q tunneling ethertype 0x9100
  service instance <number> ethernet
    encapsulation dot1q <vlan 1> [second-dot1q <vlan 2>]
    Rewrite <Rewrite>
```

**Note**
802.1q (0x8100) is the default ethertype setting.

**Note**
Cisco IOS Release 12.2(33)SRE adds support for custom ethertype to port-channels.

Supported Rewrite Rules for a Custom Ethertype Configuration

Rewriting allows you to add or remove VLAN tags in the packets transferred between two customer sites in the service provider networks.

The following types of Rewrites are supported on a Network Network Interface (NNI):
- Non-Range on C-Tag on NNI
- Range on C-Tag on NNI

Supported Rewrites for Non-Range on C-Tag with a NNI

When Custom Ethertype is configured within the NNI physical interface and VLAN range is not specified, the following Rewrites are supported for a provider bridge:
- For “encapsulation untagged”:
  - No Rewrite
  - Rewrite ingress tag push dot1q <vlan1> [second-dot1q <vlan2>] symmetric
- For “encapsulation default”:
  - No Rewrite
- For “encapsulation dot1q <vlan>”:
  - No Rewrite
  - Rewrite ingress tag pop 1 symmetric
  - Rewrite ingress tag translate 1-to-1 dot1q <vlan> symmetric, and
  - Rewrite ingress tag translate 1-to-2 dot1q <vlan 1> second-dot1q <vlan 2> symmetric
- For “encapsulation dot1q <vlan1> second-dot1q <vlan2>”:
  - No Rewrite
Supported Rewrites for Range on C-Tag with a NNI

When a VLAN range is specified on the C-Tag, push Rewrites are not supported. The following Rewrites are supported for VLAN range on C-Tag:

- For “encapsulation dot1q <vlan1 – vlan2>”:
  - No Rewrite
- For “encapsulation dot1q <vlan1> second-dot1q <vlan2 – vlan3>”:
  - No Rewrite
  - Rewrite ingress tag pop 1 symmetric
  - Rewrite ingress tag translate 1-to-1 dot1q <vlan> symmetric
  - Rewrite ingress tag translate 1-to-2 dot1q <vlan 1> second-dot1q <vlan 2> symmetric
  - Rewrite ingress tag translate 2-to-1 dot1q <vlan> symmetric, and
  - Rewrite ingress tag translate 2-to-2 dot1q <vlan 1> second-dot1q <vlan 2> symmetric

Note

To avoid hierarchical provider bridges when any Custom Ethertype is configured, NNI interface does not support “ingress push” Rewrite except for “encap untagged”.

Restrictions and Usage Guidelines

When configuring Custom Ethertype, follow these restrictions and usage guidelines:

- If a custom ethertype is configured on the port-channel, the same ethertype is implicitly configured for all the other member interfaces.
- You cannot configure Custom ethertype explicitly under a member interface of a port-channel.
- An interface configured with custom ethertype cannot be a part of port-channel.
- An ES+ port configured with custom ethertype cannot become member of port-channel.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/port or interface tengigabitethernet slot/port or interface port-channel number
4. dot1q tunneling ethertype [0x9100|0x9200|0x88A8]
5. [no] service instance id [Ethernet [service-name]]
### Custom Ethertype for EVC Interfaces

**6.** [no] encapsulation untagged, dot1q [any | vlan-id[vlan-id][vlan-id]] second-dot1q [any | vlan-id[vlan-id][vlan-id]]

**7.** Rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id} 2-to-1 dot1q vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id dot1q vlan-id}} symmetric

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example: enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface gigabitethernet slot/port</td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.</td>
</tr>
<tr>
<td></td>
<td>or interface tengigabitethernet slot/port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or interface port-channel number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface gigabitethernet 4/1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>dot1q tunneling ethertype [0x9100</td>
<td>0x9200</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# dot1q tunneling</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ethertype 0x88A8</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>service instance id ethernet [service-name]</td>
<td>Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# service instance 101</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ethernet</td>
<td></td>
</tr>
</tbody>
</table>
Custom Ethertype for EVC Interfaces

### Examples

#### Single Tag Encap with Connect with Custom Ethertype Configured

In the following example, Custom Ethertype is configured on a single tag encap using the connect configuration:

```bash
Router# sh running-config int Gi1/1
//Building configuration...
interface GigabitEthernet 1/1
  no ip address
dot1q tunneling ethertype 0x9100
  no mls qos trust
  service instance 1 ethernet
  encapsulation dot1q 10

Router# sh running-config int Gi1/2
  no ip address
dot1q tunneling ethertype 0x9100
  mls qos trust dscp
  service instance 1 ethernet
  encapsulation dot1q 10

Router)# connect LC1 GigabitEthernet 1/1 1 GigabitEthernet 1/2 1
```

#### Single Tag Encap with Bridge Domain

In the following example, Custom Ethertype is configured on a single tag encap using bridge domain configuration:

```bash
Router# sh running-config int Gi1/1
interface GigabitEthernet 1/1
```
Custom Ethertype for EVC Interfaces

Chapter 4 Configuring Layer 1 and Layer 2 Features

Custom Ethertype for EVC Interfaces

no ip address
dot1q tunneling ethertype 0x9100
no mls qos trust
service instance 1 ethernet
  encapsulation dot1q 10
  bridge-domain 100
Router#sh running-config int Gi1/2
interface GigabitEthernet 1/2
  no ip address
dot1q tunneling ethertype 0x9100
  mls qos trust dscp
  service instance 1 ethernet
  encapsulation dot1q 10
  bridge-domain 100

Single Tag Encap with XConnect

In the following example, Custom Ethertype is configured on a single tag encap with xconnect configuration:

Router#sh running-config int Gi1/1
interface GigabitEthernet 1/1
  no ip address
dot1q tunneling ethertype 0x9100
  no mls qos trust
  service instance 1 ethernet
  encapsulation dot1q 10
  xconnect 3.3.3.3 10 encapsulation mpls

Router#sh running-config int Gi1/2
interface GigabitEthernet 1/2
  ip address 10.10.10.2 255.255.255.0
  no mls qos trust
  mpls label protocol ldp
  mpls ip

Custom Ethertype Support with Sub Interfaces

In this example, Custom Ethertype is configured on a sub interface. Custom Ethertype is always configured within the main physical interface and QinQ encap is configured within the subinterface.

Router#sh running-config int Gi1/1
interface GigabitEthernet 1/1
  no ip address
dot1q tunneling ethertype 0x9100
  no mls qos trust
end
interface GigabitEthernet 1/1.10
  encapsulation dot1q 10 second-dot1q 20
  ip address 20.20.20.2 255.255.255.0
end

Verification

Use the following commands to verify operations.
## Troubleshooting

Table 4-18 provides troubleshooting solutions for the Custom Ethertype feature.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error in custom ethertype programming for all the UP links</td>
<td>Use the <code>show platform npc xlif channel-id port &lt;port sram line&gt;</code> command to verify if the port-sram is programmed correctly and displays the configured ethertype. Share the output with TAC for further investigation.</td>
</tr>
<tr>
<td>Incorrect programming of custom-ethertype in a port-channel subinterface</td>
<td>Use the <code>show vlan internal usage</code> command to trace errors related to custom ethertype programming and find the internal VLAN allocated to the sub-interface. You can use the internal VLAN to verify if the XLIF entry is present in the ES40 line card. Use this to verify if the custom ethertype is properly programmed in the XLIF.</td>
</tr>
<tr>
<td>Unknown errors and events on the port channel</td>
<td>Use the <code>debug platform port-channel [event, error]</code> command to trace the port channel events and errors. Share the output with TAC for further investigation.</td>
</tr>
</tbody>
</table>

## GE LAG with LACP on UNI with Advanced Load Balancing

The GE Link Aggregation with Advanced Load Balancing feature allows the user to specify the primary and multiple backup preferred member links for the service instance. Whenever the primary member link is available (the interface is up and is part of the port-channel group), it is used as the egress interface for a given service instance. When the preferred member link is not available (the interface is down or not part of the port-channel group), a backup member link is used. If none of the backup links are available or the user has neither configured the primary or the backup links, the 7600 platform automatically selects an egress interface for the given service instance. In this case, the user has no control over the egress interface.

If primary and backup links are configured and if the primary interface goes down, one of the backup links is selected as the egress interface. At this stage, when the primary interface comes up, there is a switch back to the primary interface. The backup link is selected based on the order of the configured list of backup link IDs. The first backup link in the list is used if available, otherwise the next backup link in the list is used. This continues until an available backup link is found.
This feature only changes egress EFP traffic in the port-channel and does not affect the ingress traffic. In the case of bridge domain, ingress traffic may enter any port that has an EFP in the same bridge domain as the EFP in the port-channel. In the case of local switching (connect) and cross-connect (xconnect), ingress traffic is received at the EFP or port specified in the connect or cross-connect configuration. This feature coexists with current service instance feature support and supports the existing scale of 8000 service instance per processor (all 8000 service instances can be on one interface). This feature supports HA and SSO as well as OIR.

Restrictions and Usage Guidelines

When configuring GE Link Aggregation with Advanced Load Balancing, follow these guidelines and restrictions:

- When the user configures a link ID for a port-channel member link and configures that member link as the preferred egress link for some service instances in that port-channel, there is redistribution of traffic. The redistribution is such that:
  - Service instances that were configured to be sent over the preferred egress member link is sent over the preferred member link. This is expected behavior.
  - Redistribution of traffic for which the user has not configured preferred member link happens. The way this redistribution happens is as follows:

    For example, let's say there are 8 member links in the port-channel. The load share of the member links is allocated by the port manager as follows,
    
    Member 1—Load share bit 0, Member 2—Load share bit 1,
    Member 3—Load share bit 2, Member 4—Load share bit 3,
    Member 5—Load share bit 4, Member 6—Load share bit 5,
    Member 6—Load share bit 6, Member 7—Load share bit 7.

    Now when the user configures Member 1 with link ID 2, the port manager code now allocates load share bit 2 to member 1. So, the new assignments are,
    
    Member 1—Load share bit 2, Member 3—Load share bit 0 (The load share of other members remains the same.)

    Consider the example where the platform has chosen an egress link that has the load share bit 2. Before the user has configured the link ID = 2 for Member 1, this EFP traffic has been sent over Member 3. After the user configuration, since member 1 now has the load share bit = 2, this traffic is now be sent over member 1.

    The reverse also happens; traffic that was going through member 1 before the user configuration now goes through member 3.

Configuring GE Link Aggregation with Advanced Load Balancing

This section describes how to configure GE LAG with LACP on UNI with Advanced Load Balancing.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/port or interface tengigabitethernet slot/port
### Chapter 4  Configuring Layer 1 and Layer 2 Features

#### GE LAG with LACP on UNI with Advanced Load Balancing

4. `channel-group channel-group-number mode {active | on | passive} link id`  
5. `exit`  
6. `interface port-channel number`  
7. `[no] service instance id {Ethernet [service-name]}`  
8. `encapsulation dot1q vlan-id [second-dot1q vlan-id]`  
9. `exit`  
10. `exit`  
11. `interface port-channel number`  
12. `[no] port-channel load-balance link ID`  
13. `[no] backup link ID_list`  
14. `[no] service-instance service_instance_list`  
15. `[no] group service_group_list

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
*enable* | Enables privileged EXEC mode.  
- Enter your password if prompted.  
**Example:**  
Router# enable | |
| **Step 2**  
*configure terminal* | Enters global configuration mode.  
**Example:**  
Router# configure terminal | |
| **Step 3**  
*interface gigabitethernet slot/port*  
or  
*interface tengigabitethernet slot/port* | Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where:  
- *slot/port*—Specifies the location of the interface.  
**Example:**  
Router(config)# interface gigabitethernet 4/1 | |
| **Step 4**  
*channel-group channel-group-number mode {active | on | passive} link id* | Assigns and configures an EtherChannel interface to an EtherChannel group.  
**Example:**  
Router(config-if)# channel-group 2 mode on link 3 | |
| **Step 5**  
*exit* | Exits the current configuration mode.  
**Example:**  
Router(config-if)# exit | |
| **Step 6**  
*interface port-channel number* | Creates the port-channel interface.  
**Example:**  
Router(config)# interface port-channel 11 | |
### GE LAG with LACP on UNI with Advanced Load Balancing

#### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>service instance id {Ethernet service-name}</td>
<td>Creates a service instance (an instantiation of a service instance) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# service instance 101 ethernet</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>encapsulation dot1q vlan-id [second-dot1q vlan-id</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# encapsulation dot1q 10</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>exit</td>
<td>Exits the current configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# exit</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>exit</td>
<td>Exits the current configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>interface port-channel number</td>
<td>Creates the port-channel interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface port-channel 11</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>[no] port-channel load-balance link ID</td>
<td>Configures the specified member link interfaces for load-balancing the port-channel's egress traffic and enters the load-balancing configuration submode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# port-channel load-balance link 3</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>[no] backup link ID_list</td>
<td>Configures a list of member links to use as backup for the primary load-balancing member link. You can create multiple backup links using the backup link command. The backup links are used in order of configuration if a Port-channel member is down. A default platform algorithm is used to find the backup links if all the configured backup links are down.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-lb)# backup link 7</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>[no] service-instance service_instance_list</td>
<td>Defines the set of service Ethernet instances whose traffic should egress over the member link identified by configuration in Step 12.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-lb)# service-instance 10</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>[no] group service_group_list</td>
<td>Defines the Ethernet service groups that will be load-balanced over an interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-lb)# group 10</td>
<td></td>
</tr>
</tbody>
</table>
Example

The following example shows four member links across two different channel-groups:

```console
Router(config)# interface Gi0/1
Router(config-if)# channel-group 1 mode on link 3

Router(config)# interface Gi0/2
Router(config-if)# channel-group 1 mode on link 4

Router(config)# interface Gi0/3
Router(config-if)# channel-group 2 mode on link 3

Router(config)# interface Gi0/4
Router(config-if)# channel-group 2 mode on link 7

Router(config)# interface Port-channel1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1Q 10
Router(config-if-srv)# service instance 20 ethernet
Router(config-if-srv)# encapsulation dot1Q 20
Router(config-if-srv)# service instance 60 ethernet
Router(config-if-srv)# group 10
Router(config-if-srv)# service instance 70 ethernet
Router(config-if-srv)# group 10

Additional service instance definitions follow:

Router(config-if)# port-channel load-balance link 3
Router(config-if-lb)# backup link 4
Router(config-if-lb)# service-instance 10,20-22
Router(config-if-lb)# port-channel load-balance link 4
Router(config-if-lb)# service-instance 30-40
Router(config-if-lb)# group 10

Router(config)# interface Port-channel2
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1Q 10
Router(config-if)# port-channel load-balance link 3
Router(config-if-lb)# backup link 7
Router(config-if-lb)# service-instance 10
```

Verification

Use the following commands to verify operation.

<table>
<thead>
<tr>
<th>Table 4-19</th>
<th>Commands for Displaying Traffic Storm Control Status and Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td><code>Router# show ethernet service instance interface interface load-balance</code></td>
<td>Displays the current egress member-link assignments for service instances configured with port-channel load-balancing.</td>
</tr>
<tr>
<td><code>Router# show ethernet service instance id efp interface port-channel group detail</code></td>
<td>Displays detailed status for the specified service instance, including the egress member-link assignment, if any.</td>
</tr>
</tbody>
</table>
Troubleshooting Load Balancing Features

Table Table 4-20 provides troubleshooting solutions for the LoadBalancing features.

Table 4-20 Troubleshooting Scenarios

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link group creation command is rejected with an error message “Incomplete command”.</td>
<td>Re-configure the link group with the specific link ID and these keywords:</td>
</tr>
<tr>
<td></td>
<td>• port-channel load-balance link:&lt;&lt; Missing link ID&gt;&gt;</td>
</tr>
<tr>
<td></td>
<td>• no port-channel load-balance link: &lt;&lt; Missing link ID&gt;&gt;</td>
</tr>
<tr>
<td></td>
<td>• default port-channel load-balance link:&lt;&lt; Missing link ID</td>
</tr>
<tr>
<td></td>
<td>• port-channel load-balance:&lt;&lt; Missing 'link' keyword</td>
</tr>
<tr>
<td></td>
<td>• port-channel: &lt;&lt; Missing 'load-balance' keyword&gt;&gt;</td>
</tr>
<tr>
<td>Error message “Invalid input detected”.</td>
<td>Re-configure the link group with valid IDs.</td>
</tr>
<tr>
<td>Back up link command is rejected and an error message displayed</td>
<td>Ensure that:</td>
</tr>
<tr>
<td></td>
<td>• The back up link ID does not overlap with the primary link ID.</td>
</tr>
<tr>
<td></td>
<td>• You have not exceeded the permissible number of back up links.</td>
</tr>
<tr>
<td></td>
<td>• You have not entered a sub-mode command in a deleted load-balance group.</td>
</tr>
<tr>
<td>Invalid input</td>
<td>Execute the show run command to confirm if duplicate back up link IDs exists between two link groups.</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the configured EFPs have valid IDs.</td>
</tr>
<tr>
<td></td>
<td>• Ensure that you have not configured an existing EFP ID in a different link group.</td>
</tr>
<tr>
<td>Member link is disabled</td>
<td>Use the show etherchannel port-channel command to verify the load share of each member link. Study the derived output and share the information with TAC for further investigation.</td>
</tr>
<tr>
<td>Traffic is not distributed equally among all members (Port channel load balancing issue)</td>
<td>Use the show ethernet service instance interface port-channel load-balance command to verify the load balancing information for all the port channels. Share the output with TAC for further investigation.</td>
</tr>
<tr>
<td>Traffic is not distributed equally among all members (EFP load balancing issues)</td>
<td>Use the show ethernet service instance id efp interface port-channel group detail command to verify and display the load balancing information for the EFPs. Share the output with TAC for further investigation.</td>
</tr>
</tbody>
</table>
Storm Control on Switchports and Ports Having EVCs

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic storm control feature prevents LAN ports from being disrupted by a broadcast or multicast traffic storm on physical interfaces. The traffic storm control level is set as a percentage of the total available bandwidth of the port.


This feature implements a mechanism to detect and control broadcast/multicast congestion/storm scenario via rate control mechanism in ES line cards.

Storm control for ES20 and ES+ cards is supported on:

- Switchports

  Note  Layer 3 (routed port) to Layer 2 (switchport) conversion is allowed only when there are no subinterfaces configured on the port.

- Ports with EVC configurations

  The feature is per port, not per EVC. Hence, all EVCs under the port are subject to the same storm control rate.

In Cisco IOS Release 15.0(1)S, the following storm control feature enhancements are covered on 67xx, 6196, ES20 and ES+ line cards:

- Port-channel interfaces: Support for port-channel interfaces on ES20 and ES+ line cards.
- Shutdown: When a storm is detected and the storm traffic exceeds the accepted threshold, the affected interface moves to error disable state. The traffic threshold is calculated as a percentage of the total bandwidth of the port (%BW). Use the error disable detection and the recovery feature, or the shut or no shut command to re-enable the port on the affected interface.
- Trap: An SNMP trap can be sent when a storm is detected.

Detecting a Broadcast Storm

A broadcast storm is detected when the following occurs:

- The port receives multicast and broadcast traffic beyond its configured bandwidth.
- The value of the TotalSuppDiscards counter increments. This value is displayed when you use the show interface gigabitEthernet <slot/port> counters storm-control command.

Restrictions and Usage Guidelines

Use the following guidelines and restrictions while configuring traffic storm control:

  Note  These restrictions and usage guidelines apply only to the Cisco 7600 Series ES+ line cards.

- Traffic storm control is disabled by default.
• Unicast storm control is not supported.
• Storm control on Layer 3 interfaces is not supported on SRD or SRE.
• Storm control feature cannot be configured at the EVC Level.
• Storm control rate can not be specified in Packets/Second (PPS).
• The broadcast and multicast suppression share the same suppression rate, therefore, when you configure a different rate either for broadcast or multicast the new rate will apply to broadcast and multicast.
• Storm control feature is not supported on the member interfaces of a port channel.
• Untagged frames can be subjected to storm control by having a service instance which marks all untagged frames. Once such a service instance is created, these frames behave like any storm control on any other EVC.
• Specify the level as a percentage of the total interface bandwidth:
  – The level can be from 0 to 100.
  – The optional fraction of a level can be from 0 to 99.
  – 100 percent means no traffic storm control.
  – 0.0 percent suppresses all traffic.
  – You can specify the percentage rate to allow in units of 0.01%.
• The maximum storm control rate is 4 Gbps (on 10 Gigabit interfaces it can be 40% of line rate)
• Storm control works in switchport dot1q-tunnel mode.
• When storm control is applied on an interface that has an inbound Layer 2 ACL applied, all packets are dropped irrespective of the configured suppression level.
• Any additions or changes made to the storm control configuration on the port-channel interface is automatically updated across all the port-channel member-links.
• Storm control configuration or deletion is not allowed on member-links.
• You can add an interface to a port-channel if the storm control configuration on the interface and the port-channel are alike.
  – You can either club member-links to form a port-channel and then configure the port-channel or change the storm control configuration on the interface to match with the port-channel, before adding it to the port-channel.
• Using the default interface command twice, removes the storm control feature from a member-link interface.
• Storm control is supported on ES+ line cards on routed or L3 interfaces from Release 15.0(1)S onwards.
• Except for BPDUs (STP), traffic storm control does not differentiate between control traffic and data traffic. For Cisco Discovery Protocol (CDP) or VLAN Trunk Protocol (VTP), a multicast suppression level of 0% suppresses even CDP or VTP packets although STP BPDUs are not suppressed by storm control.

Configuring Storm Control on Ports with EVC Configurations

This section describes how to configure storm control on ports with EVC configurations.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/port or interface tengigabitethernet slot/port
4. [no] service instance id {Ethernet service-name}
5. encapsulation dot1q vlan-id
6. [no] bridge-domain bridge-id
7. storm-control {broadcast | multicast} level level[.level]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>interface gigabitethernet slot/port or interface tengigabitethernet slot/port</td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• slot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td>4</td>
<td>[no] service instance id Ethernet service-name</td>
<td>Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td>5</td>
<td>encapsulation dot1q vlan-id</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
</tbody>
</table>
Example

This example shows a configuration for ports with EVCs on them:

Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 4/1
Router(config-if)# service instance 2 ethernet
Router(config-if-srv)# encapsulation dot1q 20
Router(config-if-srv)# bridge-domain 10
Router(config-if-srv)# storm-control multicast level 45

Configuring Storm Control on Switchports

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/port or interface tengigabitethernet slot/port
4. switchport
5. switchport mode {access | dot1q-tunnel | dynamic {auto | desirable} | private-vlan | trunk}
6. storm-control {broadcast | multicast} level level[.level]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4 Configuring Layer 1 and Layer 2 Features

Storm Control on Switchports and Ports Having EVCs

Command | Purpose
---|---
Step 3 **interface gigabitethernet slot/port** or **interface tengigabitethernet slot/port** | Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where:
- `slot/port`—Specifies the location of the interface.

Example:
Router(config)# interface gigabitethernet 4/1

Step 4 **switchport** | Sets the switching characteristics of the Layer 2-switched interface.

Example:
Router(config-if)# switchport

Step 5 **switchport mode** (`access` | `dot1q-tunnel` | `dynamic` `auto` | `desirable` | `private-vlan` | `trunk`) | Sets the interface type.

Example:
Router(config-if)# switchport mode trunk

Step 6 **storm-control** (`broadcast` | `multicast`) **level** `level` | Sets the storm control suppression level.

Example:
Router(config-if)# storm-control broadcast level 30

Example

This example shows a configuration for ports with switchport configuration:

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 4/1
Router(config)# switchport
Router(config)# switchport mode trunk
Router(config)# storm-control multicast level 45
```

Configuring Storm Control on Port Channels

Perform the following tasks to configure storm control on port channels:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `snmp-server enable traps storm-control trap-rate` `trap-rate`
4. `interface type slot/bay/port`
5. `storm-control {([broadcast | multicast] level level | action [shutdown | trap]}`
6. `end`
7. `show interfaces type/slot/port counters storm-control`
**Chapter 4      Configuring Layer 1 and Layer 2 Features**

**Storm Control on Switchports and Ports Having EVCs**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# enable</td>
</tr>
<tr>
<td>Purpose:</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | configure terminal |
| Example: | Router# configure terminal |
| Purpose: | Enters global configuration mode. |

| **Step 3** | snmp-server enable traps storm-control trap-rate trap-rate |
| Example: | Router(config)# snmp-server enable traps storm-control trap-rate 2 |
| Purpose: | (Optional) Enables SNMP storm control trap parameters. The trap-rate range is 0 to 1000 traps per minute. However, the number of traps generated for storm control cannot exceed six per minute (by design). |

| **Step 4** | interface type slot/bay/port |
| Example: | Router(config)# interface port-channel 1/0/18 |
| Purpose: | Selects an interface to configure. |

| **Step 5** | storm-control { { broadcast | multicast } level level | action (shutdown | trap) } |
| Example: | Router(config-if)# storm-control broadcast level 50  |
| Example: | Router(config-if)# storm-control action shutdown  |
| Purpose: | Sets the broadcast and multicast suppression level for traffic storm control on the interface. Enables an action for traffic storm control the interface, such as, shuts down an interface or sends an SNMP trap. However, broadcast or multicast level suppression must be enabled before setting the action. |
| Note: | A suppression level of 100% means no suppression will occur and 0% suppression means no traffic of the suppressed type will be allowed. |
| Note: | The no form of the command disables storm control for broadcast or multicast traffic or disables the specified storm-control action, on the selected interface. |
| Note: | Unicast level traffic suppression is not supported on port channel interface. |

| **Step 6** | end |
| Purpose: | Exits the configuration mode. |

| **Step 7** | show interfaces type/slot/port counters storm-control |
| Example: | Router# show interfaces gigabitEthernet 4/1 counters storm-control |
| Purpose: | Displays the total number of packets (%) discarded for the three traffic storm control levels (broadcast, multicast and unicast) on the specified interface. Displays the statistics for the TotalSuppDiscards counter. This counter increments whenever a traffic storm occurs. |

For more information regarding the commands, see the following command reference guides:

- Cisco IOS Interface and Hardware Component Command Reference
- Cisco IOS Network Management Command Reference
Example

The following is a sample configuration for storm control on a Layer 2 port channel on the ES+ line card:

```cisco
interface Port-channel22
  switchport
  switchport trunk encapsulation dot1q
  switchport mode trunk
  storm-control broadcast level 0.01
  storm-control multicast level 0.01
  storm-control action shutdown
  storm-control action trap
interface GigabitEthernet2/13
  switchport
  switchport mode trunk
  storm-control broadcast level 0.01
  storm-control multicast level 0.01
  storm-control action shutdown
  storm-control action trap
channel-group 22 mode on
interface GigabitEthernet2/21
  switchport
  switchport mode trunk
  storm-control broadcast level 0.01
  storm-control multicast level 0.01
  storm-control action shutdown
  storm-control action trap
channel-group 22 mode on
```

Use the `show interfaces interface counters storm-control` command to display the total suppression percentage of packets for the broadcast, multicast and unicast storm control traffic on all interfaces or on a specified interface. The storm control shutdown on an interface depends on the ‘TotalSuppDiscards’ counter (displayed in the example). This counter increments when a traffic storm occurs.

```cisco
Router# show interfaces counters storm-control

<table>
<thead>
<tr>
<th>Port</th>
<th>UcastSupp %</th>
<th>McastSupp %</th>
<th>BcastSupp %</th>
<th>TotalSuppDiscards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/2</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/3</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/4</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/5</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/6</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/7</td>
<td>100.00</td>
<td>20.00</td>
<td>20.00</td>
<td>2943374677</td>
</tr>
<tr>
<td>Gi1/8</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/9</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/10</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/11</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/12</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/13</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/14</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/15</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/16</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/17</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/18</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>434529474</td>
</tr>
<tr>
<td>Gi1/19</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/20</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/21</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/22</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>499018427</td>
</tr>
<tr>
<td>Gi1/23</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/24</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Storm Control on Switchports and Ports Having EVCs

Chapter 4 Configuring Layer 1 and Layer 2 Features

Verification

Use the following commands to verify operation.

Table 4-21 Commands for Displaying Traffic Storm Control Status and Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show interfaces {{type¹ slot/port}</td>
<td>switchport}</td>
</tr>
<tr>
<td>Router# show interfaces {{type¹ slot/port}</td>
<td>counters storm-control}</td>
</tr>
<tr>
<td>Router# show interfaces counters storm-control [module slot_number]</td>
<td></td>
</tr>
</tbody>
</table>

1. type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet
Storm Control over EVC

Storm control prevents traffic on a LAN from being disrupted by a broadcast, a multicast, or a unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic, and degrading network performance.

Currently for ports where EVCs are configured, storm control can be configured per port. When you configure storm control on a port, policing is applied on all the traffic on that port. Each EVC in a port represents different types of customers such as different businesses or business and individuals on the same port. When a traffic storm occurs, all traffic on the port is blocked impacting customers on all the EVCs. To prevent this, service providers need to combine similar types of customers on the same port.

Effective with Cisco IOS 15.2(2)S, storm control is supported on EVCs and policing can be applied at the EVC level. This feature enables service providers to combine different type of customers on the same port.

Restrictions for Storm Control over EVC

Following restrictions apply to storm control over EVC:

- Storm control over EVC can be configured on connect, cross connect and bridge-domain interfaces.
- Storm control is supported on port channel EVCs.
- Storm control over EVC can be configured only for broadcast or multicast packets, not for unicast packets.
- If storm control is already configured at the port level, you cannot configure storm control over EVC and vice versa.
- When an EVC moves to the error-disable state, auto-recovery can be configured for storm-control after a certain pre-determined interval.
- Storm control over EVC is supported only on the Cisco 7600 ES+ line card.
- SNMP trap is not supported.
- If storm control is enabled on a port channel EVC, the configuration is applied per network processor (NP).
- Only 256 policer profiles are supported per network processor.
- QoS and storm-control share the same hardware policer resources.

Configuring Storm Control over EVC

Perform these steps to configure storm control over EVC feature.

Summary Steps

1. enable
2. configure terminal
3. interface type number
   or
   interface port-channel number
4. service instance id ethernet
5. encapsulation dot1q \textit{vlan-id}
6. storm control \{\textit{broadcast | multicast} cir \textit{cirq action shutdown}\}
7. bridge-domain \textit{bridge-id}
8. end

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. If prompted, enter your password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: Router# enable</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: Router# configure terminal</td>
</tr>
<tr>
<td>3</td>
<td>interface gigabitethernet \textit{slot/port} or interface tengigabitethernet \textit{slot/port} or interface port-channel \textit{number}</td>
<td>Specifies the gigabit ethernet or the ten gigabit ethernet interface, or port channel to configure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\textbullet\ slot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\textbullet\ number— Specifies the port channel interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: Router(config)# interface gigabitethernet 4/1</td>
</tr>
<tr>
<td>4</td>
<td>service instance id \textit{Ethernet [service-name]}</td>
<td>Creates a service instance (an instantiation of an EVC) on the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: Router(config-if)# service instance 101 ethernet</td>
</tr>
<tr>
<td>5</td>
<td>encapsulation dot1q \textit{vlan-id}</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: Router(config-if-srv)# encapsulation dot1q 100</td>
</tr>
<tr>
<td>6</td>
<td>bridge-domain \textit{bridge-id}</td>
<td>Binds the service instance to a bridge domain instance where \textit{bridge-id} is the identifier.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: Router(config-subif)# bridge-domain 12</td>
</tr>
</tbody>
</table>
Chapter 4 Configuring Layer 1 and Layer 2 Features

Storm Control over EVC

**Note**

When the ingress packets exceed the configured rate, the EVC moves to error-disable state if the action is configured as shutdown. You can configure the EVC to move to up state after a certain interval using `errdisable recovery cause storm-control interval` command. The accepted interval varies from 30 to 86400 seconds.

### Examples

This example shows how to configure storm control over an EVC.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 200
Router(config-if-srv)# storm-control broadcast cir 11000000
```

This example shows how to configure storm control over a port channel EVC.

```
Router# enable
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 200
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# storm-control multicast cir 11000000
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Step 7</strong></td>
</tr>
<tr>
<td>`storm-control {broadcast</td>
<td>multicast} cir cir-value</td>
</tr>
<tr>
<td>Example:</td>
<td>Example:</td>
</tr>
<tr>
<td><code>Router(config-if)# storm-control broadcast cir 11000000</code></td>
<td><code>Router(config-if)# storm-control broadcast cir 11000000</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Example:</td>
</tr>
<tr>
<td><code>Router(config-if)# end</code></td>
<td><code>Router(config-if)# end</code></td>
</tr>
<tr>
<td><strong>cir-value</strong></td>
<td><strong>cir-value</strong></td>
</tr>
<tr>
<td>The acceptable range is 10000000-1000000000 for a gigabit ethernet interface, and 100000000-10000000000 for a ten gigabit interface. The recommended maximum value is up to 98 percent.</td>
<td>The acceptable range is 10000000-1000000000 for a gigabit ethernet interface, and 100000000-10000000000 for a ten gigabit interface. The recommended maximum value is up to 98 percent.</td>
</tr>
</tbody>
</table>

**Command Purpose**

- `storm-control`: Sets the storm control rate for broadcast or multicast.
- `action shutdown`: Enables an action for traffic storm control on the interface, such as, shutting down an interface.
- `cir-value`: The acceptable range is 10000000-1000000000 for a gigabit ethernet interface, and 100000000-10000000000 for a ten gigabit interface. The recommended maximum value is up to 98 percent.
Verification

Use the `show ethernet service instance id id interface type slot/port stats` command to verify the storm control over EVC configuration.

Router# show ethernet service instance id 1204 interface gigabit ethernet 2/7 stats
Port maximum number of service instances: 8000
Service Instance 1204, Interface GigabitEthernet2/7
   Pkts In  Bytes In  Pkts Out  Bytes Out
   2262238  452447600     150570   30114000
StormControl Discard Pkts: 1809909

Asymmetric Carrier-Delay

During redundant link deployments where the remote network element is enabled, a link or port may be displayed as up before the port or link is ready to forward data. This anomaly leads to traffic loss during switchover as up events are notified faster than the required routing protocol convergence time. With existing conventional carrier delay, both up and down events are notified within equal time that might not be feasible in certain network deployments. Asymmetric carrier-delays ensure stable topologies compared to conventional carrier-delay implementation.

Table 4-22 lists the differences between the conventional carrier-delay and asymmetric carrier-delay implementations.

<table>
<thead>
<tr>
<th>Table 4-22  Conventional Carrier-delay versus Asymmetric Carrier-delay</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Conventional carrier-delay implementation</strong></td>
</tr>
<tr>
<td>You can configure carrier-delay on a main physical interface.</td>
</tr>
<tr>
<td>The default value for configuring symmetric carrier delay is 10 milliseconds.</td>
</tr>
<tr>
<td>For ES+ GE linecards:</td>
</tr>
<tr>
<td>• up time is 300 milliseconds.</td>
</tr>
<tr>
<td>• down time is 10 milliseconds.</td>
</tr>
<tr>
<td>You can configure a single delay value used by both up and down events.</td>
</tr>
<tr>
<td>Traffic losses and timer optimization issues due to single configurable delay values for both up and down events.</td>
</tr>
</tbody>
</table>

Restrictions and Usage Guidelines

- The minimum valid carrier-delay down time that user can configure is 11 milliseconds for Gigabit ports. By default, carrier-delay is configured to 10 milliseconds during a card bootup. However, even if you configure a value less than 11 milliseconds, there will not be any impact on the carrier delay.
Configuring Layer 1 and Layer 2 Features

Asymmetric Carrier-Delay

- As the fast link feature and carrier-delay features are mutually exclusive, fast link feature is enabled by default.
- If you configure carrier-delay values, fast link feature is disabled on a line card.
- Though the fast link feature is configured by default in the card, the carrier-delay feature overwrites the fast link feature when configured.
- If you have not configured the carrier-delay values, fast link feature values are utilized for down event notification.

Note

If you are using Cisco IOS release version 12.2(33) SRE or prior versions and asymmetric carrier delay is configured on the interface, the show running-config command may display carrier-delay msec 0. This issue is fixed in Cisco IOS 15.0(1)S and further releases.

Configuring Asymmetric Carrier Delay

Perform these steps to configure asymmetric carrier delay.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type/ slot/port
4. carrier-delay [{up | down} [seconds][msec | sec]]
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type/ slot/port</td>
<td>Selects the main interface to configure.</td>
</tr>
<tr>
<td>Example: Router(config)# interface gigabit ethernet 8/0/14</td>
<td></td>
</tr>
</tbody>
</table>
Manual Load Balancing for EVC over Port-Channel/LACP

The Manual Load Balancing for EVC over Port-Channel/LACP feature allows the user to specify the primary and multiple backup preferred member links for the service instance. Whenever the primary member link is available (the interface is up and is part of the port-channel group), it is used as the egress interface for a given service instance. When the preferred member link is not available (the interface is down or not part of the port-channel group), a backup member link is used. If none of the backup links are available or the user has neither configured the primary or the backup links, the 7600 platform automatically selects an egress interface for the given service instance. In this case, the user has no control over the egress interface.

If primary and backup links are configured and if the primary interface goes down, one of the backup links is selected as the egress interface. At this stage, when the primary interface comes up, there is a switch back to the primary interface. The backup link is selected based on the order of the configured list of backup link IDs. The first backup link in the list is used if available, otherwise the next backup link in the list is used. This continues until an available backup link is found.

This feature only changes egress EFP traffic in the port-channel and does not affect the ingress traffic. In the case of bridge domain, ingress traffic may enter any port that has an EFP in the same bridge domain as the EFP in the port-channel. In the case of local switching (connect) and cross-connect.

### Verification

You can use the `show run` command to display the carrier-delay configurations on an ES+ physical interface. The first example shows asymmetric carrier-delay configuration and the second example shows symmetric carrier delay configuration.

```
Router# show running-config interface GigabitEthernet 8/0/4
Building configuration...
Current configuration:
!
interface GigabitEthernet8/0/4
no ip address
carrier-delay up 300
carrier-delay down 10
shutdown

Router# show running-config interface GigabitEthernet 2/0/1
Building configuration...
Current configuration:
!
interface GigabitEthernet2/0/1
no ip address
carrier-delay msec 10
shutdown
```
Manual Load Balancing for EVC over Port-Channel/LACP

When configuring Manual Load Balancing for EVC over Port-Channel/LACP, follow these guidelines and restrictions:

- When the user configures a link ID for a port-channel member link and configures that member link as the preferred egress link for some service instances in that port-channel, there is redistribution of traffic. The redistribution is such that:
  - Service instances that were configured to be sent over the preferred egress member link is sent over the preferred member link. This is expected behavior.
  - Redistribution of traffic for which the user has not configured preferred member link happens. The way this redistribution happens is as follows:

For example, let’s say there are 8 member links in the port-channel. The load share of the member links is allocated by the port manager as follows,

Member 1—Load share bit 0, Member 2—Load share bit 1,
Member 3—Load share bit 2, Member 4—Load share bit 3,
Member 5—Load share bit 4, Member 6—Load share bit 5,
Member 6—Load share bit 6, Member 7—Load share bit 7.

Now when the user configures Member 1 with link ID 2, the port manager code now allocates load share bit 2 to member 1. So, the new assignments are,

Member 1—Load share bit 2, Member 3—Load share bit 0 (The load share of other members remains the same.)

Consider the example where the platform has chosen an egress link that has the load share bit 2. Before the user has configured the link ID = 2 for Member 1, this EFP traffic has been sent over Member 3. After the user configuration, since member 1 now has the load share bit = 2, this traffic is now be sent over member 1.

The reverse also happens; traffic that was going through member 1 before the user configuration now goes through member 3.

Configuring Manual Load Balancing for EVC over Port-Channel/LACP

This section describes how to configure manual load balancing for EVC over Port-Channel/LACP.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/port or interface tengigabitethernet slot/port
4. channel-group channel-group-number mode { active | on | passive } link id
5. exit
6. `interface port-channel number`

7. `[no] service instance id {Ethernet [service-name]}

8. `encapsulation dot1q vlan-id [second-dot1q vlan-id]

9. `exit`

10. `exit`

11. `interface port-channel number`

12. `[no] port-channel load-balance link ID`

13. `[no] backup link ID_list`

14. `[no] service-instance service_instance_list`

15. `[no] group service_group_list`

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
| Example: | Router# enable  
| | • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
| Example: | Router# configure terminal |
| **Step 3** interface gigabitethernet slot/port or interface tengigabitethernet slot/port | Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where:  
| Example: | Router(config)# interface gigabitethernet 4/1  
| | • slot/port—Specifies the location of the interface. |
| **Step 4** channel-group channel-group-number mode {active | on | passive} link id | Assigns and configures an EtherChannel interface to an EtherChannel group.  
| Example: | Router(config-if)# channel-group 2 mode on link 3 |
| **Step 5** exit | Exits the current configuration mode.  
| Example: | Router(config-if)# exit |
| **Step 6** interface port-channel number | Creates the port-channel interface.  
| Example: | Router(config)# interface port-channel 11 |
### Command Purpose

#### Step 7

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no] service instance id Ethernet [service-name]</code></td>
<td>Creates a service instance (an instantiation of a service instance) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if)# service instance 101 ethernet
```

#### Step 8

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation dot1q vlan-id [second-dot1q vlan-id]</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if-srv)# encapsulation dot1q 10
```

#### Step 9

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits the current configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if-srv)# exit
```

#### Step 10

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits the current configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if)# exit
```

#### Step 11

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface port-channel number</code></td>
<td>Creates the port-channel interface.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config)# interface port-channel 11
```

#### Step 12

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no] port-channel load-balance link ID</code></td>
<td>Configures the specified member link interfaces for load-balancing the port-channel's egress traffic and enters the load-balancing configuration submode.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if)# port-channel load-balance link 3
```

#### Step 13

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no] backup link ID_list</code></td>
<td>Configures a list of member links to use as backup for the primary load-balancing member link.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if-lb)# backup link 7
```

#### Step 14

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no] service-instance service_instance_list</code></td>
<td>Defines the set of service Ethernet instances whose traffic should egress over the member link identified by configuration in Step 12.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if-lb)# service-instance 10
```

#### Step 15

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no] group service_group_list</code></td>
<td>Defines the Ethernet service groups that will be load-balanced over an interface.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-if-lb)# group 10
```
**Example**

The following example shows four member links across two different channel-groups:

```
Router(config)# interface Gi0/1
Router(config-if)# channel-group 1 mode on link 3

Router(config)# interface Gi0/2
Router(config-if)# channel-group 1 mode on link 4

Router(config)# interface Gi0/3
Router(config-if)# channel-group 2 mode on link 3

Router(config)# interface Gi0/4
Router(config-if)# channel-group 2 mode on link 7

Router(config)# interface Port-channel1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1Q 10
Router(config-if-srv)# service instance 20 ethernet
Router(config-if-srv)# encapsulation dot1Q 20
Router(config-if-srv)# service instance 60 ethernet
Router(config-if-srv)# group 10
Router(config-if-srv)# service instance 70 ethernet

Additional service instance definitions follow:

Router(config-if)# port-channel load-balance link 3
Router(config-if-lb)# backup link 4
Router(config-if-lb)# service-instance 10,20-22
Router(config-if-lb)# port-channel load-balance link 4
Router(config-if-lb)# service-instance 30-40
Router(config-if-lb)# group 10

Router(config)# interface Port-channel2
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1Q 10
Router(config-if)# port-channel load-balance link 3
Router(config-if-lb)# backup link 7
Router(config-if-lb)# service-instance 10
```

**Verification**

Use the following commands to verify operation.

**Table 4-23  Commands for Displaying Traffic Storm Control Status and Configuration**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ethernet service instance interface interface load-balance</td>
<td>Displays the current egress member-link assignments for service instances configured with port-channel load-balancing.</td>
</tr>
<tr>
<td>Router# show ethernet service instance id efp interface port-channel group detail</td>
<td>Displays detailed status for the specified service instance, including the egress member-link assignment, if any.</td>
</tr>
</tbody>
</table>
EVC Port Channel Per Flow Load Balancing

EVC port channel per flow load balancing is implemented to load balance traffic across member links of a port channel when EVCs are configured. If this type of load balancing is not configured, EVCs configured on a port channel are statically mapped to one of the active port-channel member links, which results in the outgoing traffic being limited to the bandwidth of the member link.

In a flow based load balancing on EVC port channel, different flows of traffic over an EVC interface are identified based on the data packet header. For example, the source and destination address of the data packet can be used to identify a flow. The various data traffic flows are then mapped to the different member links of a port channel. After the mapping is complete, the data traffic is transmitted through the assigned member link. The flow mapping is dynamic and changes when there is any change in the state of a member link to which a flow is assigned. The flow mappings can also change if member links are added or removed from the EVC interface. Multiple flows can be mapped to each member link.

Table 4-24 lists the ACL support for EVC port channel with per-flow load balancing.

<table>
<thead>
<tr>
<th>ACL Type</th>
<th>Ingress Support</th>
<th>Egress Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Layer 3 and Layer 4</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Ingress ACLs are internally configured on every member interface because the traffic can enter any of the member links. Therefore, the load balancing algorithm does not change the way the ingress ACLs behave.

When per-flow load balancing is configured on the port-channel, traffic for an EVC can exit from any of the member links. Therefore, with the per-flow load balancing feature enabled on the port channel, the egress ACL is internally configured on each of the member links in the egress direction. When the per-flow load balancing configuration is removed from the port-channel interface, the egress ACL information is internally removed from each active member link, and configured on the member selected by the load balancing algorithm.

Restrictions

Following restrictions apply for EVC port channel per flow load balancing:

- When flow-based load balancing is configured, bandwidth of the port channel should be configured such that it is equal to the member link’s port bandwidth. Use the `bandwidth bandwidth_value` command in the port-channel interface.
- EVC port channel per flow load balancing is supported over connect and cross connect.
- EVC port channel per flow load balancing is not supported over a bridge domain.
- Flow based load balancing cannot co-exist with other load balancing schemes.
---

If you configure QoS on a EVC port channel, QoS policies are installed on each port channel member link with the same QoS configuration of the EVC port channel. For example, if you configure 1 Mbps bandwidth on a EVC port channel with four active member links, 1 Mbps is configured on each member link.

- If EVCs within a port-channel interface are part of a service group with EVCs and sub interfaces configured, you cannot remove the flow-based load balancing configuration.
- EVC port channel per flow load balancing is done on MAC source and destination, and VC label.

### Configuring EVC Port Channel Per Flow Load Balancing

This section describes how to configure flow based load balancing on EVC port channel.

#### Summary Steps

1. `enable`
2. `configure terminal`
3. `interface port-channel channel-number`
4. `port-channel load-balance flow-based`
5. `end`

#### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface port-channel channel-number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface port-channel 1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>port-channel load-balance flow-based</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# port-channel load-balance flow-based</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
</tbody>
</table>
Example

This example shows configuring flow based load balancing on a port channel interface.

```
Router# enable
Router# configure terminal
Router(config)# interface Port-channel 1
Router(config-if)# bandwidth 1000000
Router(config-if)# port-channel load-balance flow-based
Router(config-if)# end
```

Verification

Use the `show running-config interface port-channel channel-number` command to verify the EVC port channel per flow load balancing configuration.

```
Router# enable
Router# configure terminal
Router(config)# interface Port-channel 2
Router(config-if)# port-channel load-balance flow-based
Router(config-if)# bandwidth 1000000
Router(config-if)# end
Router# show running-config interface Port-channel 2
Building configuration...
Current configuration : 113 bytes
!
interface Port-channel2
  bandwidth 1000000
  no ip address
  port-channel load-balance flow-based
end
```

Configuring Layer 3 and Layer 4 ACLs

This section describes how to configure Layer 3 and Layer 4 ACLs on an EVC port channel with per flow load balancing.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface port-channel channel-number
4. mtu bytes
5. no ip address
6. port-channel load-balance flow-based
7. service instance id ethernet [evc-name]
8. encapsulation dot1q vlan-id
### EVC Port Channel Per Flow Load Balancing

9. `ip access-group {access-list-name | access-list-number} {in | out}`

10. `xconnect peer-ip-address vc-id {encapsulation mpls}`

11. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode. Enter your password if prompted.  
**Example:**  
Router# enable |
| **Step 2** configure terminal | Enters global configuration mode.  
**Example:**  
Router# configure terminal |
| **Step 3** interface port-channel channel-number | Creates the port-channel interface.  
**Example:**  
Router(config)# interface port-channel 4 |
| **Step 4** mtu bytes | Specifies the maximum transmission unit (MTU) size.  
**Example:**  
Router(config-if)# mtu 9216 |
| **Step 5** no ip address | Disables IP address processing.  
**Example:**  
Router(config-if)# no ip address |
| **Step 6** port-channel load-balance flow-based | Configures the specified port-channel interface in a flow based load-balancing mode.  
**Example:**  
Router(config-if)# port-channel load-balance flow-based |
| **Step 7** service instance id ethernet [evc-name] | Configures an ethernet service instance on an interface and enters ethernet service configuration mode.  
**Example:**  
Router(config-if)# service instance 2 ethernet |
| **Step 8** encapsulation dot1q vlan-id | Enables IEEE 802.1Q encapsulation of traffic on the specified subinterface in a VLAN.  
**Example:**  
Router(config-if-srv)# encapsulation dot1q 2 |
Chapter 4 Configuring Layer 1 and Layer 2 Features

EVC Port Channel Per Flow Load Balancing

Configuration Examples

This example shows how to configure Layer 3 and Layer 4 ACLs on an EVC port channel with per flow load balancing.

```
Router# enable
Router# configure terminal
Router(config)# interface port-channel 4
Router(config-if)# mtu 9216
Router(config-if)# no ip address
Router(config-if)# port-channel load-balance flow-based
Router(config-if)# service instance 2 ethernet
Router(config-if-srv)# encapsulation dot1q 2
Router(config-if-srv)# ip access-group acl3 out
Router(config-if-srv)# xconnect 2.2.2.2 2 encapsulation mpls
Router(config-if-srv)# end
```

Verification

Use the `show ip access-lists access-list-name` command to list the ACL configuration.

```
Router# show ip access-lists acl3
Extended IP access list acl3
  10 permit tcp any eq 1003 any eq 5003
```

Use the `show ethernet service instance id id` command to display information about ethernet customer service instances.

```
Router# show ethernet service instance id 3
interface port-channel 4 stats Port maximum number of service instances: 8000 Service Instance 3, Interface Port-channel4
  Pkts In  Bytes In  Pkts Out  Bytes Out
  0        0        14359328 1794916000
SACL permit out count: 14362672
SACL deny out count: 504376
```
Multichassis Support for LACP

Configured at the edge of a provider’s network, Multichassis Link Aggregation Control Protocol (MLACP) features performs the following actions:

- Dual-homed devices (DHD) to provide network redundancy between two or more service provider networks.
- Allows the LACP state machine and protocol to operate in a dual-homed mode.

Each switch is a point of attachments (PoA), where one PoA is active, and the other is a standby, and the active PoA executes the multichassis link aggregation group with a DHD. A virtual LACP peer on the PoA is created giving the impression that a DHD is connected to one node. Figure 4-5 shows the placement of PoAs and DHDs in an MLACP configuration.

**Figure 4-5   Placement of PoAs and DHDs in an MLACP Implementation**

The status of the PoAs during traffic relay are:

- The two PoAs form a redundancy group, and only one of the PoAs is active at any given time.
- Only two PoAs form a redundancy group; however, you can configure a maximum of 50 redundancy groups connecting to other DHDs.
- Active links exist only between a DHD and active PoAs. None of the links between the DHD and the standby PoA relay traffic other than Bridge Protocol Data Unit (BPDU)s.
- The state of the etherchannel interface on a standby PoA is UP.

A switchover from an active PoA to a standby PoA occurs when there is a failure on the:

- Uplink port on the DHD
- Downlink port on an active PoA
- Active PoA node
Chapter 4 Configuring Layer 1 and Layer 2 Features

Multichassis Support for LACP

- Active PoA uplinks

The default switchover mechanism uses dynamic port priority changes on the port channel and member link(s) to provide revertive mode and nonrevertive mode options. The default operation in a multichassis LACP is revertive.

**Bruteforce** is a switchover mechanism where the member link is in an err-disable state after a switchover. To recover the port channel and enable the member link on a new standby PoA, use the `err disable recovery cause mlacp-minlink` command in the global configuration mode.

Use the `lacp max-bundle` command on all the PoAs to operate in the PoA control and shared control modes. The max-bundle value argument should not be less than the total number of links in the Link Aggregation Group (LAG) that are connected to the PoA. Each PoA may be connected to the DHD with a different number of links for the LAG and, therefore, configured with a different value for the max-bundle value argument.

**Note**
The `lacp failover brute-force` command cannot be used with a nonrevertive configuration.

Requirements and Restrictions

Follow these requirements and restrictions when configuring the MLACP feature in a ES40 line card:

- Supported only on ES20 and ES40 line cards, all member links on a port-channel should be on same type of line card.
- Cisco IOS Release 12.2(33)SRE supports service instances only on an MLACP port-channel.
- A PoA may be active for one port-channel, and standby for a different port-channel.
- The maximum number of port-channels supported on a PoA is 256.
- In any LACP configuration, ensure that the numerical value of the system-priority of the virtual LACP instance on the PoAs is lower (higher priority) than that on the DHD for all control variants.
- It is not recommended to configure different max bundle configurations on a PoA. For example, if DHD 1 to PoA has 4 links, PoA2 should also have 4 links.
- Links can be successfully aggregated based on the following constraints:
  - Links should be from the same line card type.
  - QoS should be validated.
  - Port-channel hashing should be identical for two links.
  - Flowcontrol should match.
- When Cisco 7600 routers are used to form a redundancy group within a PoA, the member links should adhere to the constraints listed in the previous paragraph. These constraints are not validated across PoAs and you should ensure that configuration between the two PoAs are identical.
- Ensure that the etherchannel usage configuration is identical on the two PoAs.
- The maximum bundle value on a PoA is 8.
- A maximum of two PoAs in a redundancy group and 50 redundancy groups per node are supported.
- Multiple Spanning Tree (MST) on an EVC is not supported on MLACP etherchannel ports.
- Reverse Layer 2 Gateway Protocol (RL2GP) with MLACP is not supported.
• DHD port-channel cannot use Spanning Tree Protocol (STP) or Resilient Ethernet Protocol (REP) or Reverse Layer 2 Gateway Protocol (RL2GP) as a redundancy option. DHD port-channel disables the STP enabled by default.

• Subinterfaces on port-channels are not supported.

• You can configure the `channel-group` command as active and configuring the `channel-group` command as passive is not supported.

• As the `lacp direct-loadswap` command is not applicable on a PoA, member links on a PoA are not protected with links on the same PoA.

• We do not recommend you to have different bundle configurations on a DHD. For example, if DHD 1 to PoA1 has four links, DHD 1 to PoA 2 should also have the same number of links.

• Use the `port-channel min-link` command to configure each PoA with the minimum number of links. This maintains the LAG in an active state.

• The `lacp max-bundle` command must be used on all the PoAs to operate in PoA control and shared control modes. The value of the `max-bundle` should not be less than the total number of interfaces in the LAG that are connected to the PoA.

• If you use the `lacp failover` command with `brute force`, then after the switchover, the port-channel member link moves to a errdisable state. By default, the interval is 300 seconds (tunable range is 30 seconds to 300 seconds). To recover the port-channel, use the `eraddrable recovery cause mlacp-minlink` command. EVC with connect as forwarding function is not supported.

• The `lacp failover non-revertive` and `lacp failover brute-force` commands are mutually exclusive within the same port-channel.

• Connectivity Fault Management configuration on an MLACP port-channel is not permissible.

• For best switchover performance, configure LACP fast-switchover in PoAs and DHDs.

• You cannot use MLACP port-channel for IP forwarding.

• You cannot configure REP on a MLACP port-channel.

• Use the `eraddrable recovery cause mlacp-minlink` command to auto-recover the port-channel after timer expiration.

• The core interfaces in a VPLS core should be a ES20 or ES40 line card.

• When switching to MLACP mode from P-MLACP mode, ensure that you:
  - Enable max bundle configuration to have MLACP active or standby.
  - Shutdown interface on both PoA to avoid any possible traffic loop.

The recommended configuration sequence is:

- Configure interchassis group and MLACP commands.
- Configure MLACP interchassis group and other port-channel commands.
- Add member links.

While configuring MLACP, both the active and standby PoAs need to have the same Label Distribution Protocol (LDP) router ID for the proper operation of LACP. Use the `mpls ldp router-id loopback_interface force` command to configure MPLS LDP after the loopback interface is created.

**SUMMARY STEPS**

1. `enable`
2. configure terminal
3. redundancy
4. interchassis group \{number\}
5. monitor peer \{BFD\}
6. member IP \{IP address\}
7. mlacp node-id \{number\}
8. mlacp system-mac \{IP address\}
9. mlacp system-priority priority
10. backbone interface any interface
11. exit
12. interface port-channel \{port-channel number\}
13. lacp max-bundle \{max-bundle value\}
14. lacp failover \{ non-revertive | brute force \}
15. mlacp interchassis group \{group-id\}
16. backbone int member
17. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>redundancy</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# redundancy</td>
</tr>
<tr>
<td></td>
<td>Enters redundancy configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>interchassis group {number}</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(configure-red)# interchassis group 400</td>
</tr>
<tr>
<td></td>
<td>Configures an interchassis group within the redundancy configuration mode and assigns a group number.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>monitor peer {BFD}</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(configure-red)#</td>
</tr>
<tr>
<td></td>
<td>Configures the BFD option to monitor the state of the peer. The default option is route-watch.</td>
</tr>
</tbody>
</table>
### Step 6

**Command**: `member ip (IP address)`  
**Example**:  
```
Router(configure-red)# member ip 172.3.3.3
```
**Purpose**: Configures the IP address of the mlacp peer member group.

### Step 7

**Command**: `mlacp node-id (number)`  
**Example**:  
```
Router(config-r-ic)# mlacp node-id 5
```
**Purpose**: Defines the node ID to be used in the LACP port-id field. Valid value range is 0 - 7, and the value should be different from the peer values.

### Step 8

**Command**: `mlacp system-mac (address)`  
**Example**:  
```
Router(config-r-ic)# mlacp aaaa.aaaa.aaab
```
**Purpose**: Defines and advertises the system MAC address value to the MLACP members of the redundancy group.

### Step 9

**Command**: `mlacp system-priority priority`  
**Example**:  
```
Router(config-r-ic)# mlacp system-priority 100
```
**Purpose**: Defines the system priority advertised to the other MLACP members of the redundancy group. System priority values are from 1 to 65535, the default value being 32768. The assigned values should be lower than the DHD.

### Step 10

**Command**: `backbone interface any interface`  
**Example**:  
```
Router(config-r-ic)# backbone interface GigabitEthernet2/3
```
**Purpose**: Defines the backbone interface for the MLACP configuration.

### Step 11

**Command**: `exit`  
**Purpose**: Exits the redundancy mode.

### Step 12

**Command**: `interface port-channel (port-channel number)`  
**Example**:  
```
Router# interface Port-channel1
```
**Purpose**: To identify the PoA uplink failure, configure the port-channel interface or any physical interface.

### Step 13

**Command**: `lacp max-bundle (max-bundle value)`  
**Example**:  
```
Router (config-int)# lacp max-bundle 4
```
**Purpose**: Configures the max-bundle links that are connected to the PoA. The value of the `max-bundle links` argument should not be less than the total number of links in the LAG that are connected to the PoA.

### Step 14

**Command**: `lacp failover (non-revertive | brute force)`  
**Example**:  
```
P19_C7609-S(config-if)#lacp failover ?
brute-force     Brute force interface failover
non-revertive  Non revertive interface failover
```
**Purpose**: Sets the MLACP switchover to nonrevertive or brute force. Default value is revertive. If you configure brute force, a minimum link or last link failure for every MLACP failure occurs or the dynamic lag priority value is modified.
Chapter 4  Configuring Layer 1 and Layer 2 Features

Multichassis Support for LACP

The following is a configuration example for Virtual Private Wire Services (VPWS):

**ACTIVE POA**

redundancy
interchassis group 100
    monitor peer bfd
    member ip 172.3.3.3
    backbone interface GigabitEthernet2/3
    backbone interface GigabitEthernet2/4
    mlacp system-priority 200
    mlacp node-id 0
! interface Port-channel1
    no ip address
    load-interval 30
    speed nonegotiate
    port-channel min-links 4
    lacp failover brute-force
    lacp fast-switchover
    lacp max-bundle 4
    mlacp lag-priority 28000
    mlacp interchassis group 100
    service instance 2 ethernet
    encapsulation dot1q 2
    rewrite ingress tag pop 1 symmetric
    xconnect 172.2.2.2 2 pw-class mlacp
    backup peer 172.4.4.4 2 pw-class mlacp
! pseudowire-class mlacp
    encapsulation mpls
    status peer topology dual-homed
    mpls ldp graceful-restart
! interface Loopback0
    ip address 172.1.1.1 255.255.255.255
! interface GigabitEthernet2/3
    ip address 120.0.0.1 255.255.255.0
    carrier-delay msec 0
    mpls ip
    bfd interval 100 min_rx 100 multiplier 3

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 15</strong> mlacp interchassis group (group-id)</td>
<td>Specifies that the port-channel is an MLACP port-channel. The <em>group-id</em> should match the configured redundancy group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-red)#interchassis group 230</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> backbone int member</td>
<td>Sets the backbone interface member.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-red-int)# mlacp 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong> exit</td>
<td>Exits the port-channel interface mode.</td>
</tr>
</tbody>
</table>

**Examples**

The following is a configuration example for Virtual Private Wire Services (VPWS):

**ACTIVE POA**

redundancy
interchassis group 100
    monitor peer bfd
    member ip 172.3.3.3
    backbone interface GigabitEthernet2/3
    backbone interface GigabitEthernet2/4
    mlacp system-priority 200
    mlacp node-id 0
! interface Port-channel1
    no ip address
    load-interval 30
    speed nonegotiate
    port-channel min-links 4
    lacp failover brute-force
    lacp fast-switchover
    lacp max-bundle 4
    mlacp lag-priority 28000
    mlacp interchassis group 100
    service instance 2 ethernet
    encapsulation dot1q 2
    rewrite ingress tag pop 1 symmetric
    xconnect 172.2.2.2 2 pw-class mlacp
    backup peer 172.4.4.4 2 pw-class mlacp
! pseudowire-class mlacp
    encapsulation mpls
    status peer topology dual-homed
    mpls ldp graceful-restart
! interface Loopback0
    ip address 172.1.1.1 255.255.255.255
! interface GigabitEthernet2/3
    ip address 120.0.0.1 255.255.255.0
    carrier-delay msec 0
    mpls ip
    bfd interval 100 min_rx 100 multiplier 3
interface GigabitEthernet2/9
  no ip address
  speed 1000
  channel-group 1 mode active

Use the `show lacp multi-chassis group` command to display the interchassis redundancy group value and the operational LACP parameters.

MLACP-PE1# `show lacp multi-chassis group 100`
Interchassis Redundancy Group 100
Operational LACP Parameters:
  RG State: Synchronized
  System-Id: 200.000a.f331.2680
  ICCP Version: 0
  Backbone Uplink Status: Connected
  Local Configuration:
    Node-id: 0
    System-Id: 200.000a.f331.2680

Peer Information:
  State: Up
  Node-id: 7
  System-Id: 2000.0014.6a8b.c680
  ICCP Version: 0

State Flags: Active - A
  Standby - S
  Down - D
  AdminDown - AD
  Standby Reverting - SR
  Unknown - U

mLACP Channel-groups
  Channel Group  Local/Peer  Priority  Active Links  Inactive Links
  1            A/S         28000/32768   4/4            0/0

Use the `show lacp multi-chassis port-channel` command to display the interface port-channel value channel group, LAG state, priority, inactive links peer configuration, and standby links.

MLACP-PE1# `show lacp multi-chassis port-channel 1`
Interface Port-channel1
Local Configuration:
  Address: 000a.f331.2680
  Channel Group: 1
  State: Active
  LAG State: Up
  Priority: 28000
  Inactive Links: 0
  Total Active Links: 4
    Bundled: 4
    Selected: 4
    Standby: 0
    Unselected: 0

Peer Configuration:
  Interface: Port-channel1
  Address: 0014.6a8b.c680
  Channel Group: 1
  State: Standby
  LAG State: Up
  Priority: 32768
  Inactive Links: 0
  Total Active Links: 4

Bundled: 0
Use the `show mpls ldp iccp` command to display the LDP session and ICCP state information.

```
MLACP-PE1# show mpls ldp iccp
ICPM RGID Table
  iccp:
    rg_id: 100, peer addr: 172.3.3.3
    ldp_session 0x3, client_id 0
    iccp state: ICPM_ICCP_CONNECTED
    app type: MLACP
    app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM RGID Table total ICCP sessions: 1
ICPM LDP Session Table
  iccp:
    rg_id: 100, peer addr: 172.3.3.3
    ldp_session 0x3, client_id 0
    iccp state: ICPM_ICCP_CONNECTED
    app type: MLACP
    app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM LDP Session Table total ICCP sessions: 1
```

Use the `show mpls l2transport` command to display the local interface and session details, destination address, and status.

```
MLACP-PE1# show mpls l2transport vc 2
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Po1            Eth VLAN 2                 172.2.2.2       2          UP
Po1            Eth VLAN 2                 172.4.4.4       2          STANDBY
```

Use the `show etherchannel summary` command to display the status and identity of the MLACP member links.

```
MLACP-PE1# 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
--------  -----------  --------  -----------------------------------------------
  1        Po1(RU)     LACP     Gi2/9(P)    Gi2/20(P)   Gi2/31(P)
```

Use the `show lacp internal` command to display the device, port, and member-link information.

```
MLACP-PE1# show lacp internal
Flags:  S - Device is requesting Slow LACPDU
        F - Device is requesting Fast LACPDU
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
LACP port   Admin   Oper   Port   Port
```
Chapter 4 Configuring Layer 1 and Layer 2 Features

Multichassis Support for LACP

### POA2

**redundancy**

- `interchassis group 100`
- `monitor peer bfd`
- `member ip 172.1.1.1`
- `backbone interface GigabitEthernet3/3`
- `backbone interface GigabitEthernet3/5`
- `mlacp system-priority 2000`
- `mlacp node-id 7`

**interface Port-channel1**

- `no ip address`
- `load-interval 30`
- `speed nonegotiate`
- `port-channel min-links 4`
- `lacp failover brute-force`
- `lacp fast-switchover`
- `lacp max-bundle 4`
- `mlacp interchassis group 100`
- `service instance 2 ethernet`
- `encapsulation dot1q 2`
- `rewrite ingress tag pop 1 symmetric`
- `xconnect 172.2.2.2 2 pw-class mlacp`
- `backup peer 172.4.4.4 2 pw-class mlacp`
- `pseudowire-class mlacp`
- `encapsulation mpls`
- `status peer topology dual-homed`

- `mpls ldp graceful-restart`

**interface Loopback0**

- `ip address 172.3.3.3 255.255.255.255`

**interface GigabitEthernet3/2**

- `channel-group 1 mode active`

**interface GigabitEthernet3/3**

- `ip address 123.0.0.2 255.255.255.0`
- `mpls ip`
- `mpls label protocol ldp`
- `bfd interval 100 min_rx 100 multiplier 3`

Use the `show lacp multi-chassis group` command to display the LACP parameters, local configuration, status of the backbone uplink, peer information, node ID, channel, state, priority active, and inactive links.

MLACP-PE3# `show lacp multi-chassis group 100`

Interchassis Redundancy Group 100
Operational LACP Parameters:
RG State: Synchronized
System-Id: 200.000a.f331.2680
ICCP Version: 0
Backbone Uplink Status: Connected
Local Configuration:
Node-id: 7
System-Id: 2000.0014.6a8b.c680

Peer Information:
State: Up
Node-id: 0
System-Id: 200.000a.f331.2680
ICCP Version: 0

State Flags: Active - A
            Standby  - S
            Down     - D
            AdminDown- AD
            Standby Reverting - SR
            Unknown  - U

mLACP Channel-groups

<table>
<thead>
<tr>
<th>Channel Group</th>
<th>Local/Peer</th>
<th>Priority</th>
<th>Active Links</th>
<th>Inactive Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>32768/28000</td>
<td>4/4</td>
<td>0/0</td>
<td></td>
</tr>
</tbody>
</table>

Use the `show lacp multi-chassis portchannel` command to display the interface port-channel value, channel group, LAG state, priority, inactive links, and standby links.

MLACP-P43# show lacp multi-chassis port-channel 1
Interface Port-channel1
Local Configuration:
Address: 0014.6a8b.c680
Channel Group: 1
State: Standby
LAG State: Up
Priority: 32768
Inactive Links: 0
Total Active Links: 4
            Bundled: 0
            Selected: 0
            Standby: 4
            Unselected: 0

Peer Configuration:
Interface: Port-channel1
Address: 000a.f331.2680
Channel Group: 1
State: Active
LAG State: Up
Priority: 28000
Inactive Links: 0
Total Active Links: 4
            Bundled: 4
            Selected: 4
            Standby: 0
            Unselected: 0

Use the `show mpls ldp iccp` command to display the LDP session and ICCP state information.

MLACP-P43# show mpls ldp iccp
ICPM RGID Table
  iccp:
    rg_id: 100, peer addr: 172.1.1.1
    ldp_session 0x2, client_id 0
Multichassis Support for LACP

Chapter 4 Configuring Layer 1 and Layer 2 Features

iccp state: ICPM_ICCP_CONNECTED
app type: MLACP
app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM RGID Table total ICCP sessions: 1
ICPM LDP Session Table
  iccp:
    rg_id: 100, peer addr: 172.1.1.1
    ldp_session 0x2, client_id 0
    iccp state: ICPM_ICCP_CONNECTED
    app type: MLACP
    app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM LDP Session Table total ICCP sessions: 1

MLACP-PE3# show mpls l2transport vc 2

Use the show etherchannel summary command to display the status and identity of the MLACP member links.

MLACP-PE3# 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
--------------------------------- -----------------------------------------------
1 Po1(RU) LACP Gi3/2(P) Gi3/11(P) Gi3/21(P) Gi3/32(P)

Use the show lacp internal command to display the device, port, and member-link information.

MLACP-PE3# show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode
        P - Device is in Passive mode

Channel group 1
Port Flags State LACP port Admin Oper Port Port
------- ------ --- ------- ------- ------- --- -------
Gi3/2 FA    bndl-sby 32768 0x1 0x1 0xF303 0x7
Gi3/11 FA   bndl-sby 32768 0x1 0x1 0xF30C 0x5
Gi3/21 FA   bndl-sby 32768 0x1 0x1 0xF316 0x5
Gi3/32 FA   bndl-sby 32768 0x1 0x1 0xF321 0x7

Peer (MLACP-PE1) mLACP member links
Gi2/20 SA    bndl 28000 0x1 0x1 0x8215 0x3D
Gi2/31 SA    bndl 28000 0x1 0x1 0x8220 0x3D
Gi2/40 SA    bndl 28000 0x1 0x1 0x8229 0x3D
Gi2/9 SA     bndl 28000 0x1 0x1 0x820A 0x3D
The following is a configuration example for a Virtual Private Lan Service (VPLS):

Active POA

```
redundancy
interchassis group 100
  monitor peer bfd
  member ip 172.3.3.3
  backbone interface GigabitEthernet2/3
  backbone interface GigabitEthernet2/4
  mlacp system-priority 200
  mlacp node-id 0
!
interface Port-channel1
  no ip address
  speed nonegotiate
  port-channel min-links 2
  lacp fast-switchover
  lacp max-bundle 4
  mlacp lag-priority 28800
  mlacp interchassis group 100
  service instance 4000 ethernet
  encapsulation dot1q 4000
  rewrite ingress tag pop 1 symmetric
  bridge-domain 4000
!
12 vfi VPLS manual
  vpn id 4000
  neighbor 172.2.2.2 encapsulation mpls
  neighbor 172.4.4.4 encapsulation mpls
  status decoupled
!
interface Vlan4000
  xconnect vfi VPLS
!
mlacp ldp graceful-restart
!
interface Loopback0
  ip address 172.1.1.1 255.255.255.255
!
interface GigabitEthernet2/3
  ip address 120.0.0.1 255.255.255.0
  carrier-delay 0
  mpls ip
  bfd interval 100 min_rx 100 multiplier 3
!
interface GigabitEthernet2/9
  channel-group 1 mode active
!
Use the show lacp mg command to display the LACP parameters, local configuration, status of the backbone uplink, peer information, node ID, channel, state, priority active, and inactive links.
```

MLACP-PE3# show lacp multi-chassis group 100
Interchassis Redundancy Group 100

Operational LACP Parameters:
  RG State: Synchronized
  System-Id: 200.0000.f331.2680
  ICCP Version: 0
Backbone Dplink Status: Connected
Local Configuration:
Node-id: 0
System-Id: 200.000a.f331.2680

Peer Information:
State: Up
Node-id: 7
System-Id: 2000.0014.6a8b.c680
ICCP Version: 0

State Flags: Active - A
Standby - S
Down - D
AdminDown - AD
Standby Reverting - SR
Unknown - U

mLACP Channel-groups

<table>
<thead>
<tr>
<th>Channel Group</th>
<th>Local/Peer State</th>
<th>Priority</th>
<th>Active Links</th>
<th>Inactive Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A/S</td>
<td>28000</td>
<td>4/4</td>
<td>0/0</td>
</tr>
</tbody>
</table>

Use the `show lacp multi-chassis portchannel` command to display the interface port-channel value channel group, LAG state, priority, inactive links peer configuration, and standby links.

MLACP-PE1# show lacp multi-chassis port-channel 1
Interface Port-channel1
Local Configuration:
Address: 000a.f331.2680
Channel Group: 1
State: Active
LAG State: Up
Priority: 28000
Inactive Links: 0
Total Active Links: 4
Bundled: 4
Selected: 4
Standby: 0
Unselected: 0

Peer Configuration:
Interface: Port-channel1
Address: 0014.6a8b.c680
Channel Group: 1
State: Standby
LAG State: Up
Priority: 32768
Inactive Links: 0
Total Active Links: 4
Selected: 0
Standby: 4
Unselected: 0

Use the `show mpls ldp iccp` command to display the LDP session and ICCP state information.

MLACP-PE1# show mpls ldp iccp
ICPM RGID Table
iccp:
  rg_id: 100, peer addr: 172.3.3.3
  ldp_session 0x3, client_id 0
  iccp state: ICPM_ICCP_CONNECTED
  app type: MLACP
  app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM RGID Table total ICCP sessions: 1
ICPM LDP Session Table
   iccp:
      rg_id: 100, peer addr: 172.3.3.3
      ldp_session 0x3, client_id 0
      iccp state: ICPM_ICCP_CONNECTED
       app type: MLACP
       app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM LDP Session Table total ICCP sessions: 1

Use the `show mpls l2transport` command to display the local interface and session details, destination address, and the status.

```
MLACP-PE1# show mpls l2transport vc 4000
```

<table>
<thead>
<tr>
<th>Local intf</th>
<th>Local circuit</th>
<th>Dest address</th>
<th>VC ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>VFI VPLS</td>
<td>VFI</td>
<td>172.2.2.2</td>
<td>4000</td>
<td>UP</td>
</tr>
<tr>
<td>VFI VPLS</td>
<td>VFI 172.4.4.4</td>
<td>4000</td>
<td>UP</td>
<td></td>
</tr>
</tbody>
</table>

Use the `show etherchannel summary` command to display the status and identity of the MLACP member links.

```
MLACP-PE1# 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
------- ----------- ---------- -------------------------------
      1 Po1(RU)   LACP      Gi2/9(P)  Gi2/20(P)  Gi2/31(P)  Gi2/40(P)
```

Use the `show lacp internal` command to display the device, port, and member-link information.

```
MLACP-PE1# show lacp internal
```

Flags:  S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode    P - Device is in Passive mode

```
Channel group 1
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Priority</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/9</td>
<td>SA</td>
<td>bndl-act</td>
<td>28000</td>
<td>0x1</td>
<td>0x1</td>
<td>0x820A</td>
<td>0x3D</td>
</tr>
<tr>
<td>Gi2/20</td>
<td>SA</td>
<td>bndl-act</td>
<td>28000</td>
<td>0x1</td>
<td>0x1</td>
<td>0x8215</td>
<td>0x3D</td>
</tr>
<tr>
<td>Gi2/31</td>
<td>SA</td>
<td>bndl-act</td>
<td>28000</td>
<td>0x1</td>
<td>0x1</td>
<td>0x8220</td>
<td>0x3D</td>
</tr>
<tr>
<td>Gi2/40</td>
<td>SA</td>
<td>bndl-act</td>
<td>28000</td>
<td>0x1</td>
<td>0x1</td>
<td>0x8229</td>
<td>0x3D</td>
</tr>
</tbody>
</table>

Peer (MLACP-PE3) mlACP member links

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/11</td>
<td>FA</td>
<td>hot-sby</td>
<td>32768</td>
</tr>
<tr>
<td>Gi3/21</td>
<td>FA</td>
<td>hot-sby</td>
<td>32768</td>
</tr>
<tr>
<td>Gi3/32</td>
<td>FA</td>
<td>hot-sby</td>
<td>32768</td>
</tr>
<tr>
<td>Gi3/2</td>
<td>FA</td>
<td>hot-sby</td>
<td>32768</td>
</tr>
</tbody>
</table>
Configuration example on a standby PoA:

redundancy
interchassis group 100
monitor peer bfd
member ip 172.1.1.1
backbone interface GigabitEthernet3/3
backbone interface GigabitEthernet3/5
mlacp system-priority 2000
mlacp node-id 7

interface Port-channel1
no ip address
speed nonegotiate
port-channel min-links 2
lacp fast-switchover
lacp max-bundle 4
mlacp lag-priority 28800
mlacp interchassis group 100
service instance 4000 ethernet
encapsulation dot1q 4000
rewrite ingress tag pop 1 symmetric
bridge-domain 4000

interface Port-channel1
no ip address
speed nonegotiate
port-channel min-links 2
lacp fast-switchover
lacp max-bundle 4
mlacp lag-priority 28800
mlacp interchassis group 100
service instance 4000 ethernet
encapsulation dot1q 4000
rewrite ingress tag pop 1 symmetric
bridge-domain 4000

Use the show lacp multi-chassis group interchassis group number command to display the LACP parameters, local configuration, status of the backbone uplink, peer information, nodeID, channel, state, priority, active, and inactive links.

MLACP-PE3# show lacp multi-chassis group 100
Interchassis Redundancy Group 100

Operational LACP Parameters:
RG State: Synchronized
System-Id: 200.000a.f331.2680
ICCP Version: 0
Backbone Uplink Status: Connected
Local Configuration:
Node-id: 7
System-Id: 2000.0014.6a8b.c680
Peer Information:
State:        Up
Node-id:      0
System-Id:    200.000a.f331.2680
ICCP Version: 0

State Flags: Active - A
Standby - S
Down - D
AdminDown - AD
Standby Reverting - SR
Unknown - U

mLACP Channel-groups
Channel    State      Priority     Active Links   Inactive Links
Group   Local/Peer  Local/Peer     Local/Peer      Local/Peer
1        S/A     32768/28000        4/4             0/0

Use the `show lacp multi-chassis portchannel` command to display the interface port-channel value
class group, LAG state, priority, inactive links peer configuration, and standby links.

MLACP-PE3# show lacp multi-chassis port-channel 1
Interface Port-channel1
Local Configuration:
Address: 0014.6a8b.c680
Channel Group: 1
State: Standby
LAG State: Up
Priority: 32768
Inactive Links: 0
Total Active Links: 4
   Bundled: 0
   Selected: 0
   Standby: 4
   Unselected: 0

Peer Configuration:
Interface: Port-channel1
Address: 000a.f331.2680
Channel Group: 1
State: Active
LAG State: Up
Priority: 28000
Inactive Links: 0
Total Active Links: 4
   Bundled: 4
   Selected: 4
   Standby: 0
   Unselected: 0

MLACP-PE3# show mpls ldp iccp
ICPM RGID Table
iccp:
   rg_id: 100, peer addr: 172.1.1.1
   ldp_session 0x2, client_id 0
   iccp state: ICPM_ICCP_CONNECTED
   app type: MLACP
   app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM RGID Table total ICCP sessions: 1
ICPM LDP Session Table
iccp:
   rg_id: 100, peer addr: 172.1.1.1
   ldp_session 0x2, client_id 0
iccp state: ICPM_ICCP_CONNECTED
app type: MLACP
app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM LDP Session Table total ICCP sessions: 1

MLACP-PE3# show mpls l2transport vc 2

<table>
<thead>
<tr>
<th>Local intf</th>
<th>Local circuit</th>
<th>Dest address</th>
<th>VC ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>VFI VPLS</td>
<td>VFI</td>
<td>172.2.2.2</td>
<td>4000</td>
<td>UP</td>
</tr>
<tr>
<td>VFI VPLS</td>
<td>VFI 172.4.4.4</td>
<td>4000</td>
<td></td>
<td>UP</td>
</tr>
</tbody>
</table>

Use the **show etherchannel** summary command to display the status and identity of the MLACP member links.

MLACP-PE3# 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

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Po1(RU)</td>
<td>LACP</td>
<td>Gi3/2(P) Gi3/11(P) Gi3/21(P) Gi3/32(P)</td>
</tr>
</tbody>
</table>

Use the **show lacp internal** command to display the device, port, and member-link information.

MLACP-PE3# show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode  P - Device is in Passive mode

Channel group 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/2</td>
<td>FA</td>
<td>bndl-sby</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0xF303</td>
<td>0xF7</td>
</tr>
<tr>
<td>Gi3/11</td>
<td>FA</td>
<td>bndl-sby</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0xF30C</td>
<td>0x5</td>
</tr>
<tr>
<td>Gi3/21</td>
<td>FA</td>
<td>bndl-sby</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0xF316</td>
<td>0x5</td>
</tr>
<tr>
<td>Gi3/32</td>
<td>FA</td>
<td>bndl-sby</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0xF321</td>
<td>0xF7</td>
</tr>
</tbody>
</table>

Peer (MLACP-PE1) mLACP member links

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/20</td>
<td>SA</td>
<td>bndl</td>
<td>28000</td>
<td>0x1</td>
<td>0x1</td>
<td>0x8215</td>
<td>0x3D</td>
</tr>
<tr>
<td>Gi2/31</td>
<td>SA</td>
<td>bndl</td>
<td>28000</td>
<td>0x1</td>
<td>0x1</td>
<td>0x8220</td>
<td>0x3D</td>
</tr>
<tr>
<td>Gi2/40</td>
<td>SA</td>
<td>bndl</td>
<td>28000</td>
<td>0x1</td>
<td>0x1</td>
<td>0x8229</td>
<td>0x3D</td>
</tr>
<tr>
<td>Gi2/9</td>
<td>SA</td>
<td>bndl</td>
<td>28000</td>
<td>0x1</td>
<td>0x1</td>
<td>0x820A</td>
<td>0x3D</td>
</tr>
</tbody>
</table>
Pseudo MLACP Support on Cisco 7600

In dual homing, a device is connected to the network using two independent access points or points of attachments (POAs). One POA is the primary connection and the other is a standby connection that is activated in the event of a failure of the primary connection. The Multi-chassis Link Aggregation Protocol (MLACP) solution is an active and standby Provider Edge (PE) redundancy mechanism. The Pseudo MLACP (PMLACP) feature introduced in Cisco IOS release 15.1(3)S, provides a flexible dual homing redundancy mechanism where both the connections are in the active mode (active-active mode). In PMLACP implementation, a PMLACP application is implemented on the PE router. Both the POA ports are placed in active mode with manual VLAN load balancing.

PMLACP provides higher bandwidth utilization than MLACP and other active and standby link level schemes. PMLACP provides VLAN based redundancy by allowing you to configure one primary and one secondary interface pair for each member VLAN. The POAs determine which POA is active and standby for each VLAN on a Multi-Chassis Link Aggregation (MLAG) and only the active POA forwards frames for the respective VLAN. Additionally PMLACP allows maximum flexibility for the PE-CE inter operability in terms of dual-homing redundancy and failover recovery.

Figure 4-6 explains the PMLACP implementation with manual VLAN load-balancing configuration.

**Figure 4-6 PMLACP Implementation**

In the illustration, POA ports are configured for a PMLACP role, and ports are configured in active-active mode with manual VLAN load-balancing. The POAs are configured to allow certain VLANs on one of their downlinks but not the other VLANs. The POA activates its uplinks for locally active VLANs. DHD is configured to enable all VLANs on both its uplinks. Traffic from DHD is initially flooded on both uplinks until DHD learns which uplink is active for which VLANs.

**Failover Operations**

The PMLACP feature provides network resiliency by protecting against port, link, and node failures. Figure 4-7 explains the failure points in a network.
These failures can be categorized into five types.

- A—Failure of the uplink port on the DHD
- B—Failure of the ethernet link
- C—Failure of the downlink port on the POA
- D—Failure of the POA node
- E—Failure of the active POA uplinks

The failover operations are triggered by three different events.

- Access side link or port failure (failure types A- C): PMLACP on the failing POA initiates a failover to the peer for any VLANs that were active on the failed link or links. This failover is initiated by sending an MLACP port state Type Length Value (TLV) message, indicating that the port state is down.
- Node failure (failure type D): PMLACP on the surviving POA receives a node failure notification and initiates a failover of all VLANs in standby mode on all shared MLAGs.
- POA uplink failure (failure type E): The failing POA sends a message to the peer about the core isolation using the MLACP system state TLV, indicating that the POA is isolated. It will then place all VLANs in the blocking mode.

All the three failover events involve the peer POA receiving a notification of the failure. At this point the receiving standby POA completes the following steps:

1. Unblocks any of the affected VLANs which were in standby or blocked mode.
2. Sends a MAC flush message to the access side network device through a Multiple VLAN Registration Protocol (MVRP) message. This message reflects all the VLANs which are being activated only for the associated interface. When DHD receives the MVRP message, DHD responds by flushing the MAC address tables for those VLANs.
3. Triggers the core network edge MAC flushing.
Failure Recovery

PMLACP uses revertive mode after a failure recovery to support the active-active model. The reversal process is also similar to the failover process. The standby POA initiates the reversal for each VLAN by indicating that the POA is relinquishing its active role for the VLAN. This is done through an ICCP PLACP interface state TLV message, which indicates that it is no longer in active mode for the affected VLANs. Upon TLV receipt, the recovering POA unblocks the affected VLANs and triggers the MAC flushes towards access side and core side.

Revertive mode is enabled by default. If you want to choose when to trigger reversion after the failover recovery, you can configure non revertive mode. The non revertive mode is enabled by configuring the command `lacp failover non-revertive` under port channel.

Restrictions for PMLACP on Cisco 7600

Follow this restrictions and usage guidelines while configuring PMLACP.

- PMLACP is supported on ES+ and ES 20 line cards.
- PMLACP is supported on SUP 720 and RSP 720.
- PMLACP configuration on a port channel supports only service instances.
- If PMLACP is enabled on a port channel, Resilient Ethernet Protocol (REP), Spanning Tree Protocol (STP), Link Aggregation Control Protocol (LACP), VLAN Trunking Protocol (VTP), or other layer 2 control protocols are not supported.
- The ethernet VLAN color blocking needs to be configured on all VLANs under the port channel if it has EVC xconnect or MTP configured on it. Use the `ethernet vlan color-block vlan all` command for configuring it.
- Both POAs must contain the same configuration of manual-load balance VLAN list and LAG.
- The bridge-domain that is configured under a PMLACP port channel EVC should not be part of any other non PMLACP interfaces.
- Only one port channel of MLACP or PMLACP type is supported on a single redundancy group (RG). There can be one MLACP port channel and another PMLACP port channel on a single RG, but not two port channels of the same type.
- Active VLAN list configuration needs to be the same on both POAs.
- The port-channel configuration on both POAs must be the same, but port-channel members need not be the same.
- The recommended configuration sequence for PMLACP is:
  - Configure interchassis group and PMLACP commands.
  - Configure MLACP interchassis group and other port channel commands.
  - Add member links.

Configuring PMLACP on Cisco 7600

Complete the following steps to configure PMLACP on the Cisco 7600 router.
SUMMARY STEPS

1. enable
2. configure terminal
3. pseudowire-class pw-class-name
4. encapsulation mpls
5. status peer topology dual-homed
6. exit
7. l2 vfi name manual
8. vpn id vpn-id
9. neighbor remote-id encapsulation mpls
10. exit
11. redundancy
12. interchassis group number
13. monitor peer bfd
14. member IP IP-address
15. mlacp node-id number
16. mlacp system-priority priority
17. backbone interface interface
18. exit
19. interface port-channel port-channel number
20. no ip address
21. mlacp interchassis group group-id
22. mlacp mode active-active
23. mlacp load-balance primary vlan range
24. mlacp load-balance secondary vlan range
25. ethernet vlan color-block all
26. service instance id ethernet
27. encapsulation dot1q vlan id
28. rewrite ingress tag pop {1 | 2} symmetric
29. xconnect peer-id vc-id pw-class pw-class-name
or
    bridge-domain bridge-domain-id
30. backup peer peer-id vc-id pw-class pw-class-name
31. exit
32. interface vlan bridge-domain-id
33. xconnect vfi vfi-name
34. end
## Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode, and if prompted enter your password.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>3</td>
<td>pseudowire-class pw-class-name</td>
<td>Specifies the name of a pseudowire class and enters pseudowire class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Router(config)# pseudowire-class vpws</td>
</tr>
<tr>
<td>4</td>
<td>encapsulation mpls</td>
<td>Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Router(config-pw-class)# encapsulation mpls</td>
</tr>
<tr>
<td>5</td>
<td>status peer topology dual-homed</td>
<td>Enables the reflection of the attachment circuit status on both the primary and secondary pseudowires. This configuration is necessary if the peer PEs are connected to a dual-homed device.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Router(config-pw-class)# status peer topology dual-homed</td>
</tr>
<tr>
<td>6</td>
<td>exit</td>
<td>Exits pseudowire class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Router(config-pw-class)# exit</td>
</tr>
<tr>
<td>7</td>
<td>l2 vfi name manual</td>
<td>Creates a named Layer 2 Virtual Forwarding Instance (VFI) and enables the Layer 2 VFI manual configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Router(config)# l2 vfi vpls manual</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>Perform steps 7 to 10 only if you are configuring PMLACP over VPLS. Else go to step 11.</td>
</tr>
<tr>
<td>8</td>
<td>vpn id vpn-id</td>
<td>Configures a VPN ID for the VPLS domain.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Router(config-vfi)# vpn id 17</td>
</tr>
<tr>
<td>9</td>
<td>neighbor remote-id encapsulation mpls</td>
<td>Specifies the remote peering router ID, which is the IP address of the router, and the tunnel encapsulation type for the emulated VC.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Router(config-vfi)# neighbor 1.5.1.1 encapsulation mpls</td>
</tr>
</tbody>
</table>
### Pseudo MLACP Support on Cisco 7600

#### Step 10
**exit**

**Example:**
```
Router(config-vfi)# exit
```

Exits the L2 VFI manual configuration mode.

#### Step 11
**redundancy**

**Example:**
```
Router(config)# redundancy
```

Enters redundancy configuration mode.

#### Step 12
**interchassis group** number

**Example:**
```
Router(configure-red)# interchassis group 100
```

Configures an interchassis group within the redundancy configuration mode and assigns a group number.

#### Step 13
**monitor peer bfd**

**Example:**
```
Router(configure-r-ic)# monitor peer bfd
```

Configures the BFD option to monitor the state of the peer.

**Note** The `monitor peer bfd` command is optional. If this command is not specified, the default option is `route-watch`.

#### Step 14
**member ip** IP-address

**Example:**
```
Router(configure-r-ic)# member ip 172.3.3.3
```

Configures the IP address of the MLACP peer member group.

#### Step 15
**mlacp node-id** node-id

**Example:**
```
Router(config-r-ic)# mlacp node-id 5
```

Specifies the node ID to be used in the LACP port-id field.

**node-id** — Valid range is 0 - 7, and the value should be different from the peer values.

#### Step 16
**mlacp system-priority** priority

**Example:**
```
Router(config-r-ic)# mlacp system-priority 100
```

Specifies the system priority advertised to the other MLACP members of the redundancy group.

**priority** — Acceptable range is 1 to 65535. The default value is 32768. The assigned values should be lower than the DHD.

#### Step 17
**backbone interface** interface

**Example:**
```
Router(config-r-ic)# backbone interface GigabitEthernet2/3
```

Specifies the backbone interface for the MLACP configuration.

#### Step 18
**exit**

**Example:**
```
Router(config-r-ic)# exit
```

Exits the redundancy mode.

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong> exit</td>
<td>Exits the L2 VFI manual configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>exit</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> redundancy</td>
<td>Enters redundancy configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>redundancy</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> interchassis group number</td>
<td>Configures an interchassis group within the redundancy configuration mode and assigns a group number.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interchassis group 100</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> monitor peer bfd</td>
<td>Configures the BFD option to monitor the state of the peer.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>monitor peer bfd</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> member ip IP-address</td>
<td>Configures the IP address of the MLACP peer member group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>member ip 172.3.3.3</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong> mlacp node-id node-id</td>
<td>Specifies the node ID to be used in the LACP port-id field.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>mlacp node-id 5</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> mlacp system-priority priority</td>
<td>Specifies the system priority advertised to the other MLACP members of the redundancy group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>mlacp system-priority 100</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong> backbone interface interface</td>
<td>Specifies the backbone interface for the MLACP configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>backbone interface GigabitEthernet2/3</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 18</strong> exit</td>
<td>Exits the redundancy mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>exit</code></td>
</tr>
</tbody>
</table>
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td><code>interface port-channel number</code></td>
<td>Specifies the port-channel interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface Port-channel 10</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td><code>no ip address</code></td>
<td>Removes the IP address from the interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# no ip address</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td><code>mlacp interchassis group group-id</code></td>
<td>Specifies that the port-channel is an MLACP port-channel. The <code>group-id</code> should match the configured redundancy group.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# mlacp interchassis group 100</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td><code>mlacp mode active-active</code></td>
<td>Specifies the MLACP mode as active-active.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# mlacp mode active-active</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td><code>mlacp load-balance primary vlan range</code></td>
<td>Specifies the primary VLAN range for manual load balancing.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# mlacp load-balance primary vlan 100-109</td>
<td>Specifies the VLAN ID range. Values range from 1 to 4094.</td>
</tr>
<tr>
<td>24</td>
<td><code>mlacp load-balance secondary vlan range</code></td>
<td>Specifies the secondary VLAN range for manual load balancing.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# mlacp load-balance secondary vlan 110-120</td>
<td>Specifies the VLAN ID range. Values range from 1 to 4094.</td>
</tr>
<tr>
<td>25</td>
<td><code>ethernet vlan color-block all</code></td>
<td>Blocks VLANs on EVCs with connect and cross-connect devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# ethernet vlan color-block all</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td><code>service instance id ethernet</code></td>
<td>Creates a service instance on an interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# service instance 101 ethernet</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td><code>encapsulation dot1q vlan-id</code></td>
<td>Configures the encapsulation. Defines the matching criteria to be used in order to map the ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# encapsulation dot1q 100</td>
<td></td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>`rewrite ingress tag pop {1</td>
<td>2} symmetric`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# rewrite ingress tag pop 1 symmetric</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td><code>xconnect peer-id vc-id pseudowire-class pw-classname</code></td>
<td>Binds the 802.1Q VLAN attachment circuit to a virtual circuit (VC).</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>bridge-domain bridge-domain-id</code></td>
<td>Binds the attachment circuit to a pseudowire VC.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# xconnect 3.3.3.3 90 pseudowire-class vpws</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td><code>backup peer peer-id vc-id pseudowire-class pw-classname</code></td>
<td>Specifies a redundant peer for a pseudowire virtual circuit.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# backup peer 4.3.3.3 90 pseudowire-class vpws</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td><code>exit</code></td>
<td>Exits from the interface configuration mode.</td>
</tr>
<tr>
<td>32</td>
<td><code>interface vlan bridge-domain-id</code></td>
<td>Creates or accesses a dynamic switched virtual interface (SVI).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# interface vlan 201</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td><code>xconnect vfi vfi-name</code></td>
<td>Specifies the Layer 2 VFI that you are binding to the VLAN port.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# xconnect vfi vpls</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td><code>end</code></td>
<td>Exits the port-channel interface mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Examples**

This is a configuration example for PMLACP with EVC xconnect on two POAs, A and B. In this example primary VLAN range is configured as 100-109 on router A and 110-120 on router B. The VLAN range is interchanged so that the primary VLAN range of router A becomes the secondary VLAN range in router B and the secondary VLAN range of router A becomes the primary VLAN range in router B.
RouterA> enable
RouterA# configure terminal
RouterA(config)# pseudowire-class vpws
RouterA(config-pw-class)# encapsulation mpls
RouterA(config-pw-class)# status peer topology dual-homed
RouterA(config-pw-class)# exit
RouterA(config)# 12 vfi vpls manual
RouterA(config-vfi)# vpn id 100
RouterA(config-vfi)# neighbor 3.3.3.3 encapsulation mpls
RouterA(config-vfi)# exit
RouterA(config)# redundancy
RouterA(config-red)# interchassis group 100
RouterA(config-r-ic)# monitor peer bfd
RouterA(config-r-ic)# member ip 2.2.2.2
RouterA(config-r-ic)# backbone interface GigabitEthernet8/0/10
RouterA(config-r-ic)# mlacp system-priority 100
RouterA(config-r-ic)# mlacp node-id 1
RouterA(config)# interface Port-channel10
RouterA(config-if)# no ip address
RouterA(config-if)# mlacp interchassis group 100
RouterA(config-if)# mlacp mode active-active
RouterA(config-if)# mlacp load-balance primary vlan 100-109
RouterA(config-if)# mlacp load-balance secondary vlan 110-120
RouterA(config-if)# ethernet vlan color-block all
RouterA(config-if)# service instance 10 ethernet
RouterA(config-if-srv)# encapsulation dot1q 100
RouterA(config-if-srv)# rewrite ingress tag pop 1 symmetric
RouterA(config-if-srv)# xconnect 3.3.3.3 90 pseudowire-class vpws
RouterA(config-if-srv)# backup peer 4.3.3.3 91 service instance 11 ethernet
RouterA(config-if-srv)# encapsulation dot1q 101
RouterA(config-if-srv)# rewrite ingress tag pop 1 symmetric
RouterA(config-if-srv)# bridge-domain 201
RouterA(config-if-srv)# exit
RouterA(config-if)# exit
RouterA(config)# interface vlan 201
RouterA(config-if)# no shutdown
RouterA(config-if)# xconnect vfi vpls
RouterA(config-if)# end

RouterB> enable
RouterB# configure terminal
RouterB(config)# pseudowire-class vpws
RouterB(config-pw-class)# encapsulation mpls
RouterB(config-pw-class)# status peer topology dual-homed
RouterB(config-pw-class)# exit
RouterB(config)# 12 vfi vpls manual
RouterB(config-vfi)# vpn id 100
RouterB(config-vfi)# neighbor 3.3.3.3 encapsulation mpls
RouterB(config-vfi)# exit
RouterB(config)# redundancy
RouterB(config-red)# interchassis group 100
RouterB(config-r-ic)# monitor peer bfd
RouterB(config-r-ic)# member ip 1.1.1.1
RouterB(config-r-ic)# backbone interface GigabitEthernet8/0/10
RouterB(config-r-ic)# mlacp system-priority 100
RouterB(config-r-ic)# mlacp node-id 2
RouterB(config)# interface Port-channel 10
RouterB(config-if)# no ip address
RouterB(config-if)# mlacp interchassis group 100
RouterB(config-if)# mlacp mode active-active
RouterB(config-if)# mlacp load-balance primary vlan 110-120
RouterB(config-if)# mlacp load-balance secondary vlan 100-109
Pseudo MLACP Support on Cisco 7600

Chapter 4 Configuring Layer 1 and Layer 2 Features

Pseudo MLACP Support on Cisco 7600 Router

```
RouterB(config-if)# ethernet vlan color-block all
RouterB(config-if)# service instance 10 ethernet
RouterB(config-if-srv)# encapsulation dot1q 100
RouterB(config-if-srv)# rewrite ingress tag pop 1 symmetric
RouterB(config-if-srv)# xconnect 3.3.3.3 90 pseudowire-class vpws
RouterB(config-if-srv)# backup peer 4.3.3.3 91
RouterB(config-if)# service instance 11 ethernet
RouterB(config-if-srv)# encapsulation dot1q 101
RouterB(config-if-srv)# rewrite ingress tag pop 1 symmetric
RouterB(config-if-srv)# bridge-domain 201
RouterB(config-if-srv)# exit
RouterB(config-if)# exit
RouterB(config)# interface vlan 201
RouterB(config-if)# no shutdown
RouterB(config-if)# xconnect vfi vpls
RouterB(config-if)# end
```

Verification

Use the `show lacp multi-chassis load-balance port-channel number` command to verify the PMLACP configuration information on the port channel interface.

```
PE1# show lacp multi-chassis load-balance port-channel 10

Interface Port-Channel 10
   Local Configuration:
      P-MLACP Enabled: Yes
      Redundancy Group: 100
      Revertive Mode: Non-Revertive
      Primary VLANs: 4001-4002,4004-4005,4007-4010
      Secondary VLANs: 4012-4013,4015-4016,4018-4021
   Local Interface State:
      Interface ID: 10
      Port State: Up
      Primary VLAN State: Standby
      Secondary VLAN State: Standby
   Peer Interface State:
      Interface ID: 10
      Primary VLAN State: Active
      Secondary VLAN State: Active
```

Use the `show lacp multi-chassis group` command to display the interchassis redundancy group and the operational LACP parameters.

```
PE1# show lacp multi-chassis group

Interchassis Redundancy Group 100
   Operational LACP Parameters:
      RG State: Synchronized
      System-Id: 32768.001b.0de6.3080
      ICCP Version: 0
      Backbone Uplink Status: Connected
   Local Configuration:
      Node-id: 1
      System-Id: 32768.001b.0de6.3080
   Peer Information:
      State: Up
      Node-id: 2
      System-Id: 32768.f866.f2d2.6680
      ICCP Version: 0
   State Flags: Active - A
               Standby - S
```
Chapter 4  Configuring Layer 1 and Layer 2 Features

Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide

Down - D  
AdminDown - AD  
Standby Reverting - SR  
Unknown - U  

mLACP Channel-groups

<table>
<thead>
<tr>
<th>Channel</th>
<th>State</th>
<th>Priority</th>
<th>Active Links</th>
<th>Inactive Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group 10</td>
<td>A/A</td>
<td>32768/32768</td>
<td>2/2</td>
<td>0/0</td>
</tr>
</tbody>
</table>

Redundancy Group 100 (0x64)

Applications connected: mLACP, Pseudo-mLACP

Monitor mode: BFD

member ip: 2.2.2.2 "PE2", CONNECTED

ICMP neighbor: GigabitEthernet2/9, next hop 192.168.41.2, UP

mLACP state: CONNECTED

Pseudo-mLACP state: CONNECTED

backbone int GigabitEthernet8/0/9: UP (IP)

ICRM fast-failure detection neighbor table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Status</th>
<th>Type</th>
<th>Next-hop IP</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2</td>
<td>UP</td>
<td>BFD</td>
<td>192.168.41.2</td>
<td>GigabitEthernet2/9</td>
</tr>
</tbody>
</table>

Use the `show lacp multi-chassis load-balance group` command to display the PMLACP configuration information including redundancy group, link states and interface status.

PE2#sh lacp multi-chassis load-balance group

Interchassis Redundancy Group 100

RG State: Synchronized

ICMP Version: 0

Backbone Uplink Status: Connected

Local Configuration:

Node-id: 2

Peer Information:

State: Up

Node-id: 1

ICMP Version: 0

States:

Active - ACT  
Standby - SBT

Down - DN  
AdminDown - ADN

Unknown - UN  
Reverting - REV

P-mLACP Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port State</th>
<th>Local VLAN State</th>
<th>Peer VLAN State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Local</td>
<td>Primary/Secondary</td>
<td>Primary/Secondary</td>
</tr>
<tr>
<td>10</td>
<td>ADN</td>
<td>ADN/ADN</td>
<td>DN/DN</td>
</tr>
<tr>
<td>34</td>
<td>UP</td>
<td>ACT/SBY</td>
<td>ACT/SBY</td>
</tr>
</tbody>
</table>

Troubleshooting Tips

<table>
<thead>
<tr>
<th>Table 4-25</th>
<th>Troubleshooting Tips</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>debug lacp load-balance [all</td>
<td>database</td>
</tr>
</tbody>
</table>
Layer 2 Tunneling Protocol Version 3 (L2TPv3)

The L2TPv3 feature employs L2TPv3 and pseudowire (PW) technology to provide tunneling service to Ethernet traffic. The feature is developed for SUP720-3B/3BXL and RSP720 routers, which function as Provider Edge (PE) routers in the network topologies recommended by RFC3985 Pseudowire Emulation Edge-to-Edge (PWE3) architecture. L2TPv3 also supports inter-operability between the Cisco 7600 router and any standard compliant Cisco or non-Cisco device.

A L2TPv3 tunnel is a control connection between two PE routers. One L2TPv3 tunnel can have multiple data connections, and each data connection is termed as an L2TPv3 session. The control connection is used to establish, maintain, and release sessions. Each session is identified by a session ID which is unique across the entire router.

In Figure 4-8, the attachment Virtual Circuit (VC) represents a physical or a logical port that connects a Customer Edge (CE) device to a Provider Edge (PE) device. A pseudowire is defined as a VC connecting two attachment VCs, and it consists of two L2TPv3 tunnel paths, one in each direction.

Restrictions for L2TPv3

Following restrictions apply to L2TPv3:

- Layer 2 facing line card must be an L2TPv3 supporting line card.
- There must be at least one distinct L2TPv3 tunnel per Layer 2 facing linecard.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug redundancy interchassis [all</td>
<td>Enables debugging of the interchassis redundancy</td>
</tr>
<tr>
<td>application</td>
<td>error</td>
</tr>
<tr>
<td>debug mpls ldp iccp</td>
<td>Enables debugging of the Inter Chassis Control Protocol (ICCP). Use this command from the RP.</td>
</tr>
</tbody>
</table>
The L2TPv3 feature on a Cisco 7600 router is supported on ES+ and SIP 400 line cards.
The Cisco 7600 router supports only IPv4 tunnelling for the Layer 2 frames.
The L2TPv3 feature does not support configurations such as EoL2TPv3oMPLS on the encapsulating PE.
The L2TPv3 feature supports a maximum of 16,000 pseudowires.
L2TPv3 is not supported in conjunction with EVC features. L2TPv3 coexists with EVC on the same port. That is, while one sub-interface is used to tunnel dot1q tagged traffic over L2TP, another sub-interface is used to perform EVC features.
Effective with Cisco IOS release 15.1(3)S, 4000 IP tunnels are supported on ES+ line cards.
The L2TPv3 feature does not support SSO. You must enable cookies for L2TPv3 session on HA setups.

Configuring L2TPv3

Before configuring L2TPv3, ensure the following:

- Create loopback interfaces to host the local IP addresses used by the L2TP tunnels. On a 7600 router, create multiple loopback interfaces to accommodate routing protocol configuration and L2TPv3 configuration. The `mls l2tpv3 reserve` command must be configured under loopback to indicate the Layer 2 network or CE side facing interface. This interface must be on ES+ or SIP400 LC.

Complete the following steps to configure L2TPv3:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `l2tp-class name`
4. `exit`
5. `interface loopback loopback_id`
6. `ip address loopback_address mask`
7. `mls l2tpv3 reserve interface gigabitethernet slot/subslot/port`
8. `exit`
9. `pseudowire-class pseudowire-class name`
10. `encapsulation l2tpv3`
11. `protocol l2tpv3 name`
12. `ip local interface loopback loopback_id`
13. `exit`
14. `interface gigabitethernet slot/port`
15. `encapsulation dot1q vlan_id`
16. `xconnect loopback_ip vc_id encapsulation l2tpv3 pw-class pseudowire-class name`
# Layer 2 Tunneling Protocol Version 3 (L2TPv3)

17. `exit`

## Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>l2tp-class name</code></td>
<td>Creates a template of Layer 2 Tunnel Protocol (L2TP) control plane configuration settings that can be inherited by different pseudowire classes, and enters L2TP class configuration mode. <strong>Note</strong> Optionally, you can configure the command <code>hello interval</code> in the L2TP class configuration mode. It specifies the exchange interval (in seconds) used between L2TP hello packets.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>l2tp-class H-NAME</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)#l2tp-class H-NAME</code></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>exit</code></td>
<td>Exits the L2TP-class configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>exit</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-l2tp-class)# exit</code></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>interface loopback loopback_id</code></td>
<td>Creates a loopback with the specified <code>loopback_id</code>.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>interface loopback</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# interface loopback 8000</code></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>ip address loopback_address mask</code></td>
<td>Creates an IP address for the loopback.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>ip address</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# ip address 200.1.1.1 mask 255.255.255.0</code></td>
</tr>
<tr>
<td><strong>Step 7</strong> <code>mls l2tpv3 reserve interface GigabitEthernet slot/subslot/port</code></td>
<td>Reserves a loopback interface used as a source of the L2TPv3 tunnel in a particular line card and prevents it from being used across multiple line cards. <code>slot/subslot/port</code>—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>mls l2tpv3 reserve</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# mls l2tpv3 reserve interface Gig3/1 Gig3/10</code></td>
</tr>
<tr>
<td><strong>Step 8</strong> <code>exit</code></td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>exit</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# exit</code></td>
</tr>
</tbody>
</table>
## Layer 2 Tunneling Protocol Version 3 (L2TPv3)

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td><strong>pseudowire-class</strong> pseudowire-class name</td>
<td>Specifies the name of a L2TPv3 pseudowire class and enters pseudowire class configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# pseudowire-class eth8000</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><strong>encapsulation</strong> l2tpv3</td>
<td>Configures the tunnel encapsulation type and ensures that the L2TPv3 connectivity is up.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-pw-class)#encapsulation l2tpv3</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><strong>protocol</strong> l2tpv3 name</td>
<td>Defines L2TPv3 signaling protocol.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-pw-class)#protocol l2tpv3 H-NAME</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>ip local interface loopback loopback_id</td>
<td>Specifies the local PE interface, whose IP address is used as the source IP address for sending tunneled packets.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-pw-class)#ip local interface Loopback 8000</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-pw-class)# exit</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>interface gigabitethernet slot/port</td>
<td>Enters the sub interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)#interface GigabitEthernet3/4.100</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td><strong>encapsulation</strong> dot1q vlan_id</td>
<td>Configures the encapsulation by defining the matching criteria to be used in order to map ingress dot1q frames on a VLAN interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-subif)#encapsulation dot1Q 100</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>xconnect loopback_ip vc_id encapsulation l2tpv3 pw-class pseudowire-class name</td>
<td>Attaches the Layer 2 facing interfaces to the pseudowire. The virtual circuit identifier (VC_ID) used must be a unique combination on the router. The same VC_ID must be used on both PE routers.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-subif)#xconnect 100.1.1.1 80 encap l2tpv3 pw-class eth8000</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>exit</td>
<td>Exits the sub interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-subif-xconn)#exit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Examples

This example shows how to configure L2TPv3:
```
Router# enable
Router# configure terminal
Router (config)#l2tp-class H-NAME
```
Layer 2 Tunneling Protocol Version 3 (L2TPv3)

```cisco
Router (config-l2tp-class)#exit
Router (config)#interface Loopback8000
Router (config-if)#ip address 200.1.1.1 255.255.255.0
Router (config-if)#mls l2tpv3 reserve interface Gig3/1 Gig3/10
Router (config-if)#exit
Router (config)#pseudowire-class eth8000
Router (config-pw-class)#encapsulation l2tpv3
Router (config-pw-class)#protocol l2tpv3 H-NAME
Router (config-pw-class)#ip local interface Loopback8000
Router (config-pw-class)#exit
Router (config)#interface GigabitEthernet3/4.100
Router (config-subif)#encapsulation dot1Q 100
Router (config-subif)#xconnect 100.1.1.1 80 encap l2tpv3 pw-class eth8000
Router (config-subif-xconn)#exit
Router (config-subif)#exit
Router (config)#exit
```

Verification

Use the following commands to verify the L2TPv3 configuration:

```cisco
Router #show l2tp tunnel
L2TP Tunnel Information Total tunnels 2 sessions 2

<table>
<thead>
<tr>
<th>LocTunID</th>
<th>RemTunID</th>
<th>Remote Name</th>
<th>State</th>
<th>Remote Address</th>
<th>Sessn</th>
<th>L2TP Class/Count</th>
<th>VPDN Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>2101541749</td>
<td>1606300868</td>
<td>7600-3_BR</td>
<td>est</td>
<td>100.1.1.1</td>
<td>1</td>
<td>H-NAME</td>
<td></td>
</tr>
<tr>
<td>2974027542</td>
<td>2468589365</td>
<td>7600-3_BR</td>
<td>est</td>
<td>100.1.2.1</td>
<td>1</td>
<td>H-NAME</td>
<td></td>
</tr>
</tbody>
</table>

Router #show l2tp tunnel all

L2TP Tunnel Information Total tunnels 2 sessions 2

Tunnel id 2101541749 is up, remote id is 1606300868, 1 active sessions
Locally initiated tunnel
  Tunnel state is established, time since change 03:37:28
  Tunnel transport is IP (115)
  Remote tunnel name is 7600-3_BR
    Internet Address 100.1.1.1, port 0
  Local tunnel name is 7600-2_CE
    Internet Address 200.1.1.1, port 0
L2TP class for tunnel is H-NAME
Counters, taking last clear into account:
  0 packets sent, 0 received
  0 bytes sent, 0 received
Last clearing of counters never
Counters, ignoring last clear:
  0 packets sent, 0 received
  0 bytes sent, 0 received
Control Ns 33, Nr 90
Local RWS 1024 (default), Remote RWS 1024
Control channel Congestion Control is disabled
Tunnel PMTU checking enabled
Retransmission time 1, max 1 seconds
Unsent queue size 0, max 0
Resend queue size 0, max 2
Total resends 0, ZLB ACKs sent 89
Total out-of-order dropped pkts 0
Total out-of-order reorder pkts 0
Total peer authentication failures 0
Current no session pak queue check 0 of 5
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
Control message authentication is disabled

Tunnel id 2974027542 is up, remote id is 2468589365, 1 active sessions
Locally initiated tunnel
Tunnel state is established, time since change 03:37:36
Tunnel transport is IP (115)
Remote tunnel name is 7600-3_BR
  Internet Address 100.1.2.1, port 0
Local tunnel name is 7600-2-CE
  Internet Address 200.1.2.1, port 0
L2TP class for tunnel is H-NAME
Counters, taking last clear into account:
  0 packets sent, 0 received
  0 bytes sent, 0 received
Last clearing of counters never
Counters, ignoring last clear:
  0 packets sent, 0 received
  0 bytes sent, 0 received
Control Ns 35, Nr 92
Local RWS 1024 (default), Remote RWS 1024
Control channel Congestion Control is disabled
Tunnel PMTU checking enabled
Retransmission time 1, max 1 seconds
Unsent queue size 0, max 0
Resend queue size 0, max 2
Total resends 0, ZLB ACKs sent 91
Total out-of-order dropped pkts 0
Total out-of-order reorder pkts 0
Total peer authentication failures 0
Current no session pak queue check 0 of 5
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
Control message authentication is disabled

Troubleshooting Tips

For specific troubleshooting information, contact Cisco Technical Assistance Center (TAC) at this location:

Reverse L2GP for Cisco 7600

Layer 2 Gateway Ports (L2GP) is a proposed IEEE standard (802.1ah) to address the issues that arise when two independent bridged domains are connected redundantly through an arbitrary number of links. Layer 2 Gateway Ports define how the forwarding gateways are selected so that only redundant ports are blocked and there are no temporary loops. The transitions can be at least as fast as STP L2GP resolves the transient loop problem during the re-convergence as it does not require cooperation from the outside domain.

Reverse L2GP (R-L2GP) is a variation of L2GP. In case of R-L2GP, the pseudo information of the R-L2GP is transmitted by nPEs, instead of uPEs. R-L2GP provides a mechanism to send out static preconfigured BPDUs on each ring access port of nPEs to stimulate a per-access ring instantiation of the protocol. In order for this to work, the pair of nPEs are programmed to send out BPDUs on the access ring ports in such a way that they appear to be either:

- The root bridge itself (the bridge with the lowest bridge id/priority).
- The bridge with the second lowest bridge ID/priority, and with a 0 cost path to the root.
Using R-L2GP, you can statically configure the BPDUs instead of dynamic configuration.
For more information, see Configuring STP and MST at:

Restrictions and Usage Guidelines

When configuring Reverse L2GP for the Cisco 7600 router, follow these guidelines and restrictions:

- R-L2GP is not compatible with pre-standard MST. This combination is not supported.
- Use only on bridge ports.
- Because VLAN ID is required for EVC service instance to MST instance mapping, EVC service instances without any VLAN ID in the encapsulation are not supported. This includes:
  - Untagged encapsulation
  - Priority-tagged encapsulation
  - Default encapsulation
- In EVC service instance, MST runs on the encapsulation VLAN, not on the broadcast-domain VLAN.
- Service instances with multiple outer tags are not supported.
- The feature is supported only on ES20 and ES+ line cards.
- MST and R-L2GP can co-exist on the same router.
- R-L2GP does not provide any automatic detection or recovery mechanisms for BPDU data.
- MST instance zero under RL2GP must be configured before RL2GP instance is attached to a port.
- Configure MST instance zero on the same nPE pair as RL2GP instance.
- In case of EVC service instance configuration, Encap vlan and BD vlan should be part of the same MST instance to send the TCNs on the BD-Vlans.

Configuring Reverse L2GP for 7600

To enable R-L2GP on a port, you need to:

- Configure MST
- Configure RL2GP instance
- Attach RL2GP instance to a port
- Configure VPLS BPDU Pseudo Wire

Configuration of MST must be done before configuring RL2GP and attaching it to a port. For MST configuration, you need to configure:

- Provider Bridge Mode
- Hello Time
- Name
- Revision
- MSTI information (VLAN mapping, bridge priority, port priority, and cost)
• Priority Vector information (bridge ID, port ID, Root Bridge ID)

Since the R-L2GP configuration is bundled with the MSTI configuration, the above parameters can be recycled from the MSTI and MST region (currently only one MST region is supported on IOS) configurations. This section describes how to configure Reverse L2GP for 7600. It consists of the following sections:

• Configuring MST, page 4-185
• Configuring the RL2GP Instance, page 4-186
• Attaching the RL2GP Instance to a Port, page 4-187
• Configuring the VPLS Pseudo Wire, page 4-187

Configuring MST

SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree mst configuration
4. [no] name name
5. [no] revision version
6. [no] instance instance-id {vlans vlan-range}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 spanning-tree mst config</td>
<td>Enters MST-configuration submode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# spanning-tree mst configuration</td>
<td></td>
</tr>
<tr>
<td>Step 4 [no] name name</td>
<td>Sets the name of a Multiple Spanning Tree (MST) region.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-mst)# name Cisco</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the RL2GP Instance

#### SUMMARY STEPS

1. `spanning-tree pseudo-information transmit identiffer`
2. `remote-id id`
3. `mst root mac-address`
4. `mst root priority`
5. `mst root`
6. `mst cost`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configured the Reverse-L2GP configuration on the interface (or untagged EFP port).</td>
</tr>
<tr>
<td><code>spanning-tree pseudo-information transmit identiffer</code></td>
<td>configured the remote RL2GP instance Id that pairs with the specified R-L2GP instance Id.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# spanning-tree pseudo-information transmit 10</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Adds MST instance list to R-L2GP instance and configures R-L2GP root bridge MAC address for MST instance (or multiple MST instances).</td>
</tr>
<tr>
<td><code>remote-id id</code></td>
<td>Adds MST instance list to R-L2GP instance and configures the R-L2GP bridge priority (in multiples of 4096) for instances.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-pseudo)# remote-id 5</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>configured the Reverse-L2GP configuration on the interface (or untagged EFP port).</td>
</tr>
<tr>
<td><code>mst root mac-address</code></td>
<td>configured the remote RL2GP instance Id that pairs with the specified R-L2GP instance Id.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# spanning-tree pseudo-information transmit 10</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Adds MST instance list to R-L2GP instance and configures R-L2GP root bridge MAC address for MST instance (or multiple MST instances).</td>
</tr>
<tr>
<td><code>mst root priority</code></td>
<td>Adds MST instance list to R-L2GP instance and configures the R-L2GP bridge priority (in multiples of 4096) for instances.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-pseudo)# mst root priority</td>
</tr>
</tbody>
</table>
### Attaching the RL2GP Instance to a Port

#### SUMMARY STEPS

1. `interface gigabitethernet slot/port` or `interface tengigabitethernet slot/port`
2. `spanning-tree pseudo-information transmit identifier`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>interface gigabitethernet slot/port</code></td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where:</td>
</tr>
<tr>
<td>or</td>
<td>• <code>slot/port</code>—Specifies the location of the interface.</td>
</tr>
<tr>
<td><code>interface tengigabitethernet slot/port</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface gigabitethernet 4/1</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>spanning-tree pseudo-information transmit identifier</code></td>
<td>Configures the Reverse-L2GP configuration on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# spanning-tree pseudo-information transmit 10</td>
</tr>
</tbody>
</table>

### Configuring the VPLS Pseudo Wire

#### SUMMARY STEPS

1. `l2 vfi name manual`
2. `vpn id vpn_id`
3. `forward permit L2protocol all`
4. `neighbor ip-address vc-id {encapsulation mpls | pw-class pw-class-name}`
5. `exit`
6. `interface vlan vlanid type {trbrf | ethernet}`
7. `xconnect vfi vfi_name`
Reverse L2GP for Cisco 7600

Chapter 4 Configuring Layer 1 and Layer 2 Features

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>l2 vfi name manual</strong> &lt;br&gt;Example: &lt;br&gt;Router(config)# l2 vfi vfitest1 manual</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>vpn id vpg_id</strong> &lt;br&gt;Example: &lt;br&gt;Router(config-vfi)# vpn id 303</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>forward permit L2protocol all</strong> &lt;br&gt;Example: &lt;br&gt;Router(config-vfi)# forward permit L2protocol all</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**neighbor ip-address vc-id {encapsulation mpls</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>exit</strong> &lt;br&gt;Example: &lt;br&gt;Router(config-vfi)# exit</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>**interface vlan vlanid type {trbrf</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>xconnect vfi vfi name</strong> &lt;br&gt;Example: &lt;br&gt;Router(config-if)# xconnect vfi vfi16</td>
</tr>
</tbody>
</table>

Examples

This is a sample configuration for switch port:

----- PE1 configuration -----

**Step 1:**

PE1(config)#configure terminal <br>Enter configuration commands, one per line. End with CNTL/Z. <br>PE1(config)#spanning-tree mode mst <br>PE1(config)#spanning-tree extend system-id <br>PE1(config)#spanning-tree pseudo-information transmit 2 <br>PE1(config)#remote-id 1
**Step 2:**

PE1(config-pseudo)# mst 0 root 32768 0000.0000.0001
%Warning: Please make same configuration change on mst instance 0 for remote Pseudo Info instance also. Difference in mst instance 0 config on Pseudo Info pair can cause network instability
PE1(config-pseudo)# mst 1 root 32768 0000.0000.0002
PE1(config-pseudo)# mst 1 cost 100
PE1(config-pseudo)# exit
PE1(config)# spanning-tree mst configuration
PE1(config-mst)# instance 1 vlan 100-200, 400-500

**Step 3:**

PE1(config)# l2 vfi bpdupw manual
PE1(config-vfi)# vpn id 100
PE1(config-vfi)# forward permit L2protocol all
PE1(config-vfi)# neighbor 22.22.22.22 encapsulation mpls
PE1(config-vfi-neighbor)#

**Step 4:**

PE1(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE1(config)# interface Vlan1
PE1(config-if)# no ip address
PE1(config-if)# xconnect vfi bpdupw
PE1(config-if)# end
PE1#

Use the show commands to check the configuration:

PE1# show running-config int te4/1
Building configuration...
Current configuration : 119 bytes
!
interface TenGigabitEthernet4/1
switchport
switchport mode trunk
spanning-tree pseudo-information transmit 2
end

PE1# show spanning-tree mst
##### MST0 vlans mapped: 1-99,201-399,501-4094
Bridge address 0013.5f21.e240 priority 32768 (32768 sysid 0)
Root this switch for the CIST
Operational hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured hello time 2 , forward delay 15, max age 20, max hops 20

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4  Configuring Layer 1 and Layer 2 Features

Reverse L2GP for Cisco 7600

---------------                 ---- --- --------- --------
Te4/1                            Desg FWD 2000      128.769  P2p R-L2GP
PW 22.22.22.22:100                 Desg FWD 200      128.1020 P2p R-L2GP

### MST1  vlans mapped:  100-200,400-500
Bridge  address 0013.5f21.e240 priority 32769 (32768 sysid 1)
Root    this switch for MST1

Interface    Role Sts Cost  Prio.Nbr Type
----------------                 ---- --- --------- --------
----------------                 ---- --- --------- --------
Te4/1                            Desg FWD 2000      128.769  P2p R-L2GP
PW 22.22.22.22:100                 Desg FWD 200      128.1020 P2p R-L2GP

PE1# show spanning-tree pseudo-information
Pseudo id 2, type transmit:
  remote_id 1
  mst_region_id 0, port_count 1, update_flag 0x0
  mrecord 0x1DF3627C, mrec_count 2:
    msti 0: root_id 32768.0000.0000.0001, root_cost 0, update_flag 0x0
    msti 1: root_id 32769.0000.0000.0002, root_cost 100, update_flag 0x0
Pseudo interfaces:
  TenGigabitEthernet4/1

PE1# show spanning-tree mst detail
##### MST0  vlans mapped:  1-99,201-399,501-4094
Bridge  address 0013.5f21.e240 priority 32768 (32768 sysid 0)
Root    this switch for the CIST
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured hello time 2, forward delay 15, max age 20, max hops 20

TenGigabitEthernet4/1 of MST0 is designated forwarding
Port info  port id       128.769  priority 128  cost 2000
Designated root  address 0013.5f21.e240 priority 32768 cost 0
Design. regional root  address 0013.5f21.e240 priority 32768 cost 0
Designated bridge  address 0013.5f21.e240 priority 32768 port id 128.769
Pseudo-info (id 2) is running
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 500, received 0

PW 22.22.22.22:100 of MST0 is designated forwarding
Port info  port id       128.1020  priority 128  cost 200
Designated root  address 0013.5f21.e240 priority 32768 cost 0
Design. regional root  address 0013.5f21.e240 priority 32768 cost 0
Designated bridge  address 0013.5f21.e240 priority 32768 port id 128.1020
Pseudo-info (id 255) is running
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 396, received 14

##### MST1  vlans mapped:  100-200,400-500
Bridge  address 0013.5f21.e240 priority 32769 (32768 sysid 1)
Root    this switch for MST1

TenGigabitEthernet4/1 of MST1 is designated forwarding
Port info  port id       128.769  priority 128  cost 2000
Designated root  address 0013.5f21.e240 priority 32769 cost 0
Design. regional root  address 0013.5f21.e240 priority 32769 cost 0
Designated bridge  address 0013.5f21.e240 priority 32769 port id 128.769
Pseudo-info (id 2) is running
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 501, received 0
FW 22.22.22.22:100 of MST1 is designated forwarding
Port info port id 128.1020 priority 128 cost 200
Designated root address 0013.5f21.e240 priority 32769 cost 0
Designated bridge address 0013.5f21.e240 priority 32769 port id 128.1020
Pseudo-info (id 255) is running
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 396, received 13

PE1#show mpls l2transport vc detail
Local interface: VFI bpdupw VFI up
  Interworking type is Ethernet
  Destination address: 22.22.22.22, VC ID: 100, VC status: up
  Output interface: Te4/2, imposed label stack {17}
  Preferred path: not configured
  Default path: active
  Next hop: 12.0.0.2
  Create time: 00:15:59, last status change time: 00:15:35
  Signaling protocol: LDP, peer 22.22.22.22:0 up
  Targeted Hello: 11.11.11.11(LDP Id) -> 22.22.22.22, LDP is UP
  Status TLV support (local/remote): enabled/supported
  LDP route watch: enabled
  Label/status state machine: established, LruRru
  Last local dataplane status rcvd: No fault
  Last BFD dataplane status rcvd: Not sent
  Last BFD peer monitor status rcvd: No fault
  Last local AC circuit status rcvd: No fault
  Last local LDP TLV status sent: No fault
  Last remote LDP TLV status rcvd: No fault
  MPLS VC labels: local 21, remote 17
  PWID: 16424
  Group ID: local 0, remote 0
  MTU: local 1500, remote 1500
  Remote interface description:
    MAC Withdraw: sent:1, received:3
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  SSO Descriptor: 22.22.22.22/100, local label: 21
    SSM segment/switch IDs: 20523/4135 (used), PWID: 16424
  VC statistics:
    transit packet totals: receive 29, send 390
    transit byte totals: receive 4423, send 55770
    transit packet drops: receive 0, seq error 0, send 0

PE1#show vfi name bpdupw
Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No
VFI name: bpdupw, state: up, type: multipoint signaling: LDP
  VPN ID: 100
  Forwarding BPDUs only
  Bridge-Domain 1 attachment circuits:
    Vlan1
  Neighbors connected via pseudowires:
    Peer Address VC ID S
    22.22.22.22 100 Y

----- PE2 configuration -----
Chapter 4  Configuring Layer 1 and Layer 2 Features

Reverse L2GP for Cisco 7600

PE2(config)#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PE2(config)#spanning-tree mode mst
PE2(config)#spanning-tree extend system-id
PE2(config)#spanning-tree pseudo-information transmit 1
PE2(config-pseudo)# remote-id 2
PE2(config-pseudo)# mst 0 root 32768 0000.0000.0001
%Warning: Please make same configuration change on mst instance 0 for remote Pseudo Info instance also. Difference in mst instance 0 config on Pseudo Info pair can cause network instability
PE2(config-pseudo)# mst 1 root 32768 0000.0000.0002
PE2(config-pseudo)# mst 1 cost 100
PE2(config-pseudo)# exit
PE2(config)#spanning-tree mst configuration
PE2(config-mst)# instance 1 vlan 100-200, 400-500
PE2(config-mst)#end
PE2#

Step 2:

PE2(config)#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PE2(config)#interface GigabitEthernet13/7
PE2(config-if)#switchport
PE2(config-if)#switchport mode trunk
PE2(config-if)#spanning-tree pseudo-information transmit 1
PE2(config-if)#end
PE2#

Step 3:

PE2(config)#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PE2(config)#l2 vfi bpdupw manual
PE2(config-vfi)#vpn id 100
PE2(config-vfi)#forward permit L2protocol all
PE2(config-vfi)#neighbor 11.11.11.11 encapsulation mpls
PE2(config-vfi)#end
PE2#

Step 4:

PE2(config)#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PE2(config)#interface Vlan1
PE2(config-if)#no ip address
PE2(config-if)#xconnect vfi bpdupw
PE2(config-if)#end
PE2#

Use the show commands to check the configuration:

PE2(config)#show running-config int gig 13/7
Building configuration...

Current configuration : 117 bytes
!
interface GigabitEthernet13/7
  switchport
  switchport mode trunk
  spanning-tree pseudo-information transmit 1
end
PE2# show spanning-tree mst

#### MST0  vlans mapped:  1-99,201-399,501-4094
Bridge  address 0015.c7f9.cc40 priority 32768 (32768 sysid 0)
Root  this switch for the CIST
Operational hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured hello time 2 , forward delay 15, max age 20, max hops 20

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PW 11.11.11.11:100</td>
<td>Desg FWD 200</td>
<td>128.3070</td>
<td>P2p R-L2GP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi13/7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### MST1  vlans mapped:  100-200,400-500
Bridge  address 0015.c7f9.cc40 priority 32769 (32768 sysid 1)
Root  this switch for MST1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PW 11.11.11.11:100</td>
<td>Desg FWD 20000</td>
<td>128.3079</td>
<td>P2p R-L2GP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi13/7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

PE2# show spanning-tree pseudo-information

Pseudo id 1, type transmit:
  remote_id 2
  mst_region_id 0, port_count 1, update_flag 0x0
  mrecord 0x542B57F4, mrec_count 2:
    msti 0: root_id 32768.0000.0000.0001, root_cost 0, update_flag 0x0
    msti 1: root_id 32769.0000.0000.0002, root_cost 100, update_flag 0x0
Pseudo interfaces:
  GigabitEthernet13/7

PE2# show spanning-tree mst detail

#### MST0  vlans mapped:  1-99,201-399,501-4094
Bridge  address 0015.c7f9.cc40 priority 32768 (32768 sysid 0)
Root  this switch for the CIST
Operational hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured hello time 2 , forward delay 15, max age 20, max hops 20

PW 11.11.11.11:100 of MST0 is designated forwarding
Port info  port id 128.3070 priority 128 cost 200
Designated root  address 0015.c7f9.cc40 priority 32768 cost 0
Design. regional root address 0015.c7f9.cc40 priority 32768 cost 0
Designated bridge  address 0015.c7f9.cc40 priority 32768 port id 128.3070
Pseudo-info (id 255) is running
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 16, received 385

GigabitEthernet13/7 of MST0 is designated forwarding
Port info  port id 128.3079 priority 128 cost 20000
Designated root  address 0015.c7f9.cc40 priority 32768 cost 0
Design. regional root address 0015.c7f9.cc40 priority 32768 cost 0
Designated bridge  address 0015.c7f9.cc40 priority 32768 port id 128.3079
Pseudo-info (id 1) is running
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 163, received 0

#### MST1  vlans mapped:  100-200,400-500
Bridge  address 0015.c7f9.cc40 priority 32769 (32768 sysid 1)
Reverse L2GP for Cisco 7600

Root          this switch for MST1

PW 11.11.11.11:100 of MST1 is designated forwarding
Port info    port id  128.3070 priority  128 cost       200
Designated root address 0015.c7f9.cc40 priority 32769 cost 0
Designated bridge address 0015.c7f9.cc40 priority 32769 port id 128.3070
Pseudo-info (id 255) is running
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 16, received 354

GigabitEthernet13/7 of MST1 is designated forwarding
Port info    port id  128.3079 priority  128 cost      20000
Designated root address 0015.c7f9.cc40 priority 32769 cost 0
Designated bridge address 0015.c7f9.cc40 priority 32769 port id 128.3079
Pseudo-info (id 1) is running
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 164, received 0

PE2#show mpls l2transport vc detail
Local interface: VFI bpdupw VFI up
Interworking type is Ethernet
Destination address: 11.11.11.11, VC ID: 100, VC status: up
 Output interface: Te12/2, imposed label stack (21)
 Preferred path: not configured
 Default path: active
 Next hop: 12.0.0.1
Create time: 00:09:39, last status change time: 00:09:04
Signaling protocol: LDP, peer 11.11.11.11:0 up
 Targeted Hello: 22.22.22.22(LDP Id) -> 11.11.11.11, LDP is UP
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last local SSS circuit status rcvd: No fault
Last local SSS circuit status sent: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP Adj status rcvd: No fault
MPLS VC labels: local 17, remote 21
PWID: 8250
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description:
 MAC Withdraw: sent:1, received:1
Sequencing: receive disabled, send disabled
Control Word: On (configured: autosense)
SSS Descriptor: 11.11.11.11/100, local label: 17
 SSM segment/switch IDs: 16444/4153 (used), PWID: 8250
VC statistics:
 transit packet totals: receive 289, send 15
 transit byte totals: receive 41327, send 2091
 transit packet drops: receive 0, seq error 0, send 0

PE2#show vfi name bpdupw
Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No
VFI name: bpdupw, state: up, type: multipoint signaling: LDP
 VPN ID: 100
Forwarding BPDUs only
Bridge-Domain 1 attachment circuits:
 Vlan1
Neighbors connected via pseudowires:
Peer Address     VC ID     S
11.11.11.11    100        Y

This is a sample configuration for EVC-BD:

----- PE1 configuration -----

Step 1:

PE1(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE1(config)# spanning-tree mode mst
PE1(config)# spanning-tree extend system-id
PE1(config)# spanning-tree pseudo-information transmit 2
PE1(config-pseudo)# remote-id 1
PE1(config-pseudo)# mst 0 root 32768 0000.0000.0001
#Warning: Please make same configuration change on mst instance 0 for
remote Pseudo Info instance also. Difference in mst instance 0 config
on Pseudo Info pair can cause network instability
PE1(config-pseudo)# mst 1 root 32768 0000.0000.0002
PE1(config-pseudo)# mst 1 cost 100
PE1(config-pseudo)# exit
PE1(config)# spanning-tree mst configuration
PE1(config-mst)# instance 1 vlan 100-200, 400-500

Step 2:

PE1(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE1(config)# interface TenGigabitEthernet4/1
PE1(config-if)# spanning-tree pseudo-information transmit 2
PE1(config-if)# service instance 2 ethernet
PE1(config-if-srv)# encapsulation dot1q 2
PE1(config-if-srv)# rewrite ingress tag pop 1 symmetric
PE1(config-if-srv)# bridge-domain 100
PE1(config-if-srv)# service instance 499 ethernet
PE1(config-if-srv)# encapsulation dot1q 499
PE1(config-if-srv)# rewrite ingress tag pop 1 symmetric
PE1(config-if-srv)# bridge-domain 402
PE1(config-if-srv)# end
PE1#

Step 3:

PE1(config)# l2 vfi bpdupw manual
PE1(config-vfi)# vpn id 100
PE1(config-vfi)# forward permit L2protocol all
PE1(config-vfi)# neighbor 22.22.22.22 encapsulation mpls
PE1(config-vfi-neighbor)#

Step 4:

PE1(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE1(config)# interface Vlan1
PE1(config-if)# no ip address
PE1(config-if)# xconnect vfi bpdupw
PE1(config-if)# end
PE1#

Use the show commands to check the configuration:

PE1# show running-config int te4/1
Building configuration...
Current configuration : 361 bytes

! interface TenGigabitEthernet4/1
ip arp inspection limit none
no ip address
spanning-tree pseudo-information transmit 2
service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
!
  service instance 499 ethernet
  encapsulation dot1q 499
  rewrite ingress tag pop 1 symmetric
  bridge-domain 402
!
end

PE1#show spanning-tree mst

##### MST0  vlans mapped:  1-99,201-399,501-4094
Bridge address 0013.5f21.e240  priority 32768 (32768 sysid 0)
Root this switch for the CIST
Operational hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured hello time 2 , forward delay 15, max age 20, max hops 20

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te4/1</td>
<td></td>
<td></td>
<td>2000</td>
<td>128.769</td>
<td>P2p</td>
</tr>
<tr>
<td>PW 22.22.22:100</td>
<td></td>
<td></td>
<td>1022</td>
<td>128.1022</td>
<td>P2p</td>
</tr>
</tbody>
</table>

##### MST1  vlans mapped:  100-200,400-500
Bridge address 0013.5f21.e240  priority 32769 (32768 sysid 1)
Root this switch for MST1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te4/1</td>
<td></td>
<td></td>
<td>2000</td>
<td>128.769</td>
<td>P2p</td>
</tr>
<tr>
<td>PW 22.22.22:100</td>
<td></td>
<td></td>
<td>1022</td>
<td>128.1022</td>
<td>P2p</td>
</tr>
</tbody>
</table>

PE1#show spanning-tree pseudo-information
Pseudo id 2, type transmit:
  remote_id 1
  mst_region_id 0, port_count 1, update_flag 0x0
  mrecord 0x1DF3627C, mrec_count 2:
    msti 0: root_id 32768.0000.0000.0001, root_cost 0, update_flag 0x0
    msti 1: root_id 32769.0000.0000.0002, root_cost 100, update_flag 0x0
Pseudo interfaces:
  TenGigabitEthernet4/1

PE1#show spanning-tree mst configuration
Name [] Revision 0 Instances configured 2

<table>
<thead>
<tr>
<th>Instance</th>
<th>Vlans mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1-99,201-399,501-4094</td>
</tr>
<tr>
<td>1</td>
<td>100-200,400-500</td>
</tr>
</tbody>
</table>

PE1#
PE1# show spanning-tree mst detail

### MST0 vlans mapped: 1-99,201-399,501-4094
Bridge address 0013.5f21.e240 priority 32768 (32768 sysid 0)
Root this switch for the CIST
Operational hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured hello time 2 , forward delay 15, max age 20, max hops 20

TenGigabitEthernet4/1 of MST0 is designated forwarding
Port info  port id 128.769 priority 128 cost 2000
Designated root address 0013.5f21.e240 priority 32768 cost 0
Designated regional root address 0013.5f21.e240 priority 32768 cost 0
Designated bridge address 0013.5f21.e240 priority 32768 port id 128.769
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 770, received 0

FW 22.22.22.22:100 of MST0 is designated forwarding
Port info  port id 128.1022 priority 128 cost 200
Designated root address 0013.5f21.e240 priority 32769 cost 0
Designated regional root address 0013.5f21.e240 priority 32769 cost 0
Designated bridge address 0013.5f21.e240 priority 32769 port id 128.1022
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 0, received 0

### MST1 vlans mapped: 100-200,400-500
Bridge address 0013.5f21.e240 priority 32769 (32768 sysid 1)
Root this switch for MST1

TenGigabitEthernet4/1 of MST1 is designated forwarding
Port info  port id 128.769 priority 128 cost 2000
Designated root address 0013.5f21.e240 priority 32769 cost 0
Designated bridge address 0013.5f21.e240 priority 32769 port id 128.769
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 770, received 0

FW 22.22.22.22:100 of MST1 is designated forwarding
Port info  port id 128.1022 priority 128 cost 200
Designated root address 0013.5f21.e240 priority 32769 cost 0
Designated bridge address 0013.5f21.e240 priority 32769 port id 128.1022
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 0, received 0

PE1# show mpls l2transport vc detail

Local interface: VFI bdpupw VFI up
Interworking type is Ethernet
Destination address: 22.22.22.22, VC ID: 100, VC status: up
Output interface: Te4/2, imposed label stack {17}
Preferred path: not configured
Default path: active
Next hop: 12.0.0.2
Create time: 00:23:57, last status change time: 00:23:24
Signaling protocol: LDP, peer 22.22.22.22:0 up
Targeted Hello: 11.11.11.11(LDP Id) -> 22.22.22.22, LDP is UP
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Reverse L2GP for Cisco 7600

Chapter 4 Configuring Layer 1 and Layer 2 Features

Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 22, remote 17
PWID: 20498
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description:
  MAC Withdraw: sent:3, received:4
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  SSM Descriptor: 22.22.22.100, local label: 22
  SSM segment/switch IDs: 16405/12305 (used), PWID: 20498
VC statistics:
  transit packet totals: receive 0, send 129268726
  transit byte totals: receive 0, send 4504820856
  transit packet drops: receive 0, seq error 0, send 0

PE1# show vfi name bpdupw

Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No

VFI name: bpdupw, state: up, type: multipoint signaling: LDP
  VPN ID: 100
  Forwarding BPDUs only
  Bridge-Domain 1 attachment circuits:
    Vlan1
  Neighbors connected via pseudowires:
    Peer Address VC ID S
    22.22.22.22 100 Y

----- PE2 configuration -----

Step 1:

PE2(config)# spanning-tree mode mst
PE2(config)# spanning-tree extend system-id
PE2(config)# spanning-tree pseudo-information transmit 1
PE2(config)# spanning-tree pseudo-information remote-id 2
PE2(config)# mst 0 root 32768 0000.0000.0001
  Warning: Please make same configuration change on mst instance 0 for
  remote Pseudo Info instance also. Difference in mst instance 0 config
  on Pseudo Info pair can cause network instability
PE2(config)# mst 1 root 32768 0000.0000.0002
PE2(config)# mst 1 cost 100
PE2(config)# exit
PE2(config)# spanning-tree mst configuration
PE2(config-mst)# instance 1 vlan 100-200, 400-500
PE2(config-mst)# end
PE2#

Step 2:

PE2(config)# spanning-tree mode mst
PE2(config)# spanning-tree extend system-id
PE2(config)# spanning-tree pseudo-information transmit 1
PE2(config)# spanning-tree pseudo-information remote-id 2
PE2(config)# spanning-tree mst configuration
PE2(config-mst)# instance 1 vlan 100-200, 400-500
PE2(config-mst)# end
PE2#
Step 3:

PE2(config-if-srv)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE2(config)# l2 vfi bpdupw manual
PE2(config-vfi)# vpn id 100
PE2(config-vfi)# forward permit L2protocol all
PE2(config-vfi)# neighbor 11.11.11.11 encapsulation mpls
PE2(config-vfi)# end
PE2#

Step 4:

PE2(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE2(config)# interface Vlan1
PE2(config-if)# no ip address
PE2(config-if)# xconnect vfi bpdupw
PE2(config-if)# end
PE2#

Use the show commands to check the configuration:

PE2(config)# show running-config int gig 13/7
Building configuration...

Current configuration: 359 bytes
!
interface GigabitEthernet13/7
 ip arp inspection limit none
 no ip address
 spanning-tree pseudo-information transmit 1
 service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
!
 service instance 499 ethernet
  encapsulation dot1q 499
  rewrite ingress tag pop 1 symmetric
  bridge-domain 402
!
end

PE2(config)# show spanning-tree mst

### MST0 vlans mapped:  1-99,201-399,501-4094
Bridge address 0015.c7f9.cc40 priority 32768 (32768 sysid 0)
Root this switch for the CIST
Operational hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured hello time 2, forward delay 15, max age 20, max hops 20

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
</table>
---

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>PW 11.11.11.11:100</td>
<td>Desg FWD 200</td>
<td>128.3070</td>
<td>P2p</td>
<td>R-L2GP</td>
<td></td>
</tr>
<tr>
<td>Gi13/7</td>
<td>Desg FWD 20000</td>
<td>128.3079</td>
<td>P2p</td>
<td>R-L2GP</td>
<td></td>
</tr>
</tbody>
</table>

### MST1

- **vlans mapped:** 100-200,400-500
- **Bridge address:** 0015.c7f9.cc40
- **priority:** 32769 (32768 sysid 1)

**Interface Role**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>PW 11.11.11.11:100</td>
<td>Desg FWD 200</td>
<td>128.3070</td>
<td>P2p</td>
<td>R-L2GP</td>
<td></td>
</tr>
<tr>
<td>Gi13/7</td>
<td>Desg FWD 20000</td>
<td>128.3079</td>
<td>P2p</td>
<td>R-L2GP</td>
<td></td>
</tr>
</tbody>
</table>

PE2# `show spanning-tree pseudo-information`

- **Pseudo id 1, type transmit:**
  - remote_id 2
  - mst_region_id 0, port_count 1, update_flag 0x0
  - mrecord 0x542B57F4, mrec_count 2:
    - msti 0: root_id 32768.0000.0000.0001, root_cost 0, update_flag 0x0
    - msti 1: root_id 32769.0000.0000.0002, root_cost 100, update_flag 0x0

**Pseudo interfaces:**

- GigabitEthernet13/7

PE2# `show spanning-tree mst configuration`

- **Name:** [ ]
- **Revision:** 0
- **Instances configured:** 2

**Instance Vlans mapped**

<table>
<thead>
<tr>
<th>Instance</th>
<th>Vlans mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1-99,201-399,501-4094</td>
</tr>
<tr>
<td>1</td>
<td>100-200,400-500</td>
</tr>
</tbody>
</table>

PE2# `show spanning-tree mst detail`

- **### MST0 vlans mapped:** 1-99,201-399,501-4094
- **Bridge address:** 0015.c7f9.cc40
- **priority:** 32768 (32768 sysid 0)

**Operational**

- hello time 2, forward delay 15, max age 20, txholdcount 6
- hello time 2, forward delay 15, max age 20, max hops 20

**PW 11.11.11.11:100 of MST0 is designated forwarding**

**Port info**

<table>
<thead>
<tr>
<th>Port id</th>
<th>priority</th>
<th>cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.3070</td>
<td>128</td>
<td>200</td>
</tr>
</tbody>
</table>

**Designated root**

<table>
<thead>
<tr>
<th>Port id</th>
<th>priority</th>
<th>cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.3070</td>
<td>128</td>
<td>200</td>
</tr>
</tbody>
</table>

**Designated regional root**

<table>
<thead>
<tr>
<th>Port id</th>
<th>priority</th>
<th>cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.3070</td>
<td>128</td>
<td>200</td>
</tr>
</tbody>
</table>

**Designated bridge**

<table>
<thead>
<tr>
<th>Port id</th>
<th>priority</th>
<th>cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.3070</td>
<td>128</td>
<td>200</td>
</tr>
</tbody>
</table>

**Pseudo-info (id 255) is running**

**Timers:** message expires in 0 sec, forward delay 0, forward transitions 1

**Bpdus sent 0, received 0**

PE2#}

**### MST1 vlans mapped:** 100-200,400-500

**Bridge address:** 0015.c7f9.cc40

**priority:** 32769 (32768 sysid 1)
Root this switch for MST1

Port info
Designated root
Designated bridge
Pseudo-info (id 255) is running
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 0, received 0

GigabitEthernet13/7 of MST1 is designated forwarding
Port info
Designated root
Designated bridge
Pseudo-info (id 1) is running
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 1303, received 0

PE2# show mpls l2transport vc detail
Local interface: VFI bpdupw VFI up
Interworking type is Ethernet
Destination address: 11.11.11.11, VC ID: 100, VC status: up
Output interface: Te12/2, imposed label stack (17)
Preferred path: not configured
Default path: active
Next hop: 12.0.0.1
Create time: 00:10:32, last status change time: 00:09:56
Signalling protocol: LDP, peer 11.11.11.11:0 up
Targeted Hello: 22.22.22.22(LDP Id) -> 11.11.11.11, LDP is UP
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last local SSS circuit status rcvd: No fault
Last local SSS circuit status sent: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 19, remote 17
PWID: 4144
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description:
MAC Withdraw: sent:1, received:1
Sequencing: receive disabled, send disabled
Control Word: On (configured: autosense)
SSO Descriptor: 11.11.11.11/100, local label: 19
SSM segment/switch IDs: 16433/4138 (used), PWID: 4144
VC statistics:
transit packet totals: receive 0, send 0
transit byte totals: receive 0, send 0
transit packet drops: receive 0, seq error 0, send 0

PE2# show vfi name bpdupw
Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No
VFI name: bpdupw, state: up, type: multipoint signaling: LDP
VPN ID: 100
Forwarding BPDUs only
Bridge-Domain 1 attachment circuits:
Vlan1
Neighbors connected via pseudowires:
<table>
<thead>
<tr>
<th>Peer Address</th>
<th>VC ID</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.11.11.11</td>
<td>100</td>
<td>Y</td>
</tr>
</tbody>
</table>
Troubleshooting

Table 4-26 provides troubleshooting solutions for the Reverse L2GP feature.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>RL2GP configuration issues</td>
<td>Use the `show spanning-tree pseudo-information [id [configuration</td>
</tr>
<tr>
<td>Disabled STP or MST instances</td>
<td>Use the `show spanning-tree [active</td>
</tr>
</tbody>
</table>
| `spanning-tree pseudo-information transmit` command is rejected | Verify if:  
  - All MST instances within the pseudo-information are configured within the MST global configuration.  
  - MSTI 0 (IST) is configured within the pseudo-information. |
| Cannot configure MST                   | Re-configure MSTE and ensure that priority, MAC address and cost are the same on both the network processor engines. |
| System loops                           | Re-configure all the 64 VLAN instances per RL2GP within a Pseudo ID.     |
| Configuration is rejected when the MST region ID is modified. | As IOS supports only single region MST, remove the multiple MSTRegion IDs that have been configured and configure only a single MST ID. |

Configuring Static MAC Binding to EVCs and Psuedowires

Static MAC on Ethernet Flow Point (EFP) and Pseudowire (PW) provides the functionality to configure static unicast or multicast MAC address on EFP and PW. A MAC address can be statically added on an EFP under port channel. This feature provides the functionality to:

- Avoid dynamically learning the traffic in both the directions.
- Configure MAC address for Service Instance (SI) and PW.
- Limit the scope of the data traffic flood by creating multicast groups. The static MAC address assignment is important to avoid dynamically learning the traffic in both directions and also to limit the flooding scope by creating a static multicast group.
- Implement security by explicitly enabling a single MAC address.
- Resolve the problem of MAC address aging out as the dynamic learning is disabled.
- Optimize L2 table performance by limiting the table size.
- Configure static MAC on EFPs on port channels.
- Configure fully meshed pseudowire network between core facing routers and place them under single multicast group.
Restrictions and Usage Guidelines

When configuring static MAC on EFP and PW for the Cisco 7600 routers, follow these guidelines and restrictions:

- You cannot configure unicast static MAC address and MAC security on the same EFP simultaneously. For multicast addresses, static MAC and MAC security can be simultaneously supported under EFP.
- No support for static MAC on PWs on C-MAC Bridge-domain.
- Static MACs are related to a L2 Bridge-domain table, so only the bridged services are supported.
- When static MAC is configured on VPLS PW, and core-facing interface fails resulting in egress interface to move to available interface, the traffic may be delayed.
- Static MAC configuration is supported only on EVC bridge-domain interfaces and VFI pseudowires.
- Static Mac configuration on EFP is supported on ES+ and ESM20 line cards.
- Static Mac configuration on VFI PW is supported on ES+, ESM20 and SIP 400 line cards.
- Number of MACs per PW (unicast and multicast) is limited to 1024.
- Number of MACs per Bridge-domain or VFI (unicast and multicast) is limited to 1024.
- Number of MACs per system (unicast and multicast) is limited to 1024.
- A static unicast MAC can be configured either globally or within a EVC or PW, not both. If a static unicast MAC is configured within a EVC or PW first, then configuring the same MAC address globally using the command `mac-address-table static H.H.H vlan vlan_id [drop | interface]` makes the configuration within EVC or PW invalid.
- MAC security on MTP or C-MAC is not supported.

The next section describes how to configure Static MAC on EFP and PW for the Cisco 7600 router. You need to configure MPLS on core-facing router before configuring static MAC on PW. The information about configuring MPLS on core-facing router is included as a separate section.

- Configuring Static MAC over EFP for the Cisco 7600 Router, page 4-204
- Configuring MPLS on Core-Facing Interface, page 4-206
- Configuring Static MAC over Pseudowire for the Cisco 7600 Router, page 4-208

Configuring Static MAC over EFP for the Cisco 7600 Router

This section describes how to configure static MAC over EFP or SIs.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/port or interface tengigabitethernet slot/port
4. service instance id Ethernet [service-name]
5. encapsulation dot1q | untagged | double tagged | default vlan-id
6. bridge-domain bridge-id
7. mac static address mac_address [auto-learn | disable-snooping]
8. **mac static address** `mac_address`

9. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Router# enable</td>
</tr>
</tbody>
</table>
| Purpose | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Step 2** | **configure terminal**  |
| Example: | Router# Router(config)# interface gigabitethernet 4/1 |
| Purpose | Enters global configuration mode. |
| **Step 3** | **interface gigabitethernet slot/port** or **interface tengigabitethernet slot/port**  |
| Example: | Router(config)# Interface GigabitEthernet2/0/0 |
| Purpose | Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure, where slot/port specifies the location of the interface. |
| **Step 4** | **service instance id Ethernet [service-name]**  |
| Example: | Router(config-if)# service instance 101 ethernet |
| Purpose | Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode. |
| **Step 5** | **encapsulation dot1q {any | vlan-id [vlan-id]} second-dot1q {any | vlan-id[vlan-id]}**  |
| Example: | Router(config-if-srv)# encapsulation dot1q 100 second dot1q 200 |
| Purpose | Configuring the encapsulation. Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance. |
| **Step 6** | **bridge-domain bridge-id**  |
| Example: | Router(config-if-srv)# bridge-domain 12 |
| Purpose | Configuring the bridge domain. Binds the service instance to a bridge domain instance where `bridge-id` is the identifier for the bridge domain instance. |
Examples

This example shows how to configure static MAC over EFP or SIs:

```
Router# enable
Router# configure terminal
Router(config-if)# service instance 10 ethernet
Router(config-srv)# encapsulation dot1q 20
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac static address 0002.1122.0010
Router(config-if-srv)# mac static address 0100.5e00.1111 disable-snooping
Router(config-if-srv)# mac static address 0002.1122.0011 auto-learn
Router(config-if-srv)# mac static address 0100.5e00.1112
Router(config-if-srv)# mac static address 0002.1122.0012 auto-learn
Router(config-if-srv)# mac static address 0100.5e00.1113 disable-snooping
Router(config-if-srv)# exit
```

Configuring MPLS on Core-Facing Interface

You need to configure MPLS on the core-facing router before configuring static MAC over pseudowire. This section describes how to configure MPLS on the core-facing router interface.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface gigabitethernet slot/subslot/port`
4. `ip address ip_Address mask`
5. `mpls ip`
6. mpls label protocol ldp
7. exit
8. interface loopback Loopback_Id
9. ip address loopback_address mask
10. exit
11. mpls ldp router-id loopback loopback_Id force
12. router ospf ospf_Id
13. network loopback_network wildcard_mask area 0
14. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1  | enable  | Enables privileged EXEC mode.  
| Example: | Router# enable | - Enter your password if prompted. |
| Step 2  | configure terminal | Enters global configuration mode. |
| Example: | Router# configure terminal | |
| Step 3  | interface gigabitethernet slot/sub-slot/port | Specifies the Gigabit Ethernet interface to configure, where: slot/subslot/port—Specifies the location of the interface. |
| Example: | Router(config)# interface gigabitethernet 3/0/0 | |
| Step 4  | ip address ip_Address mask | Configures ip address for the interface. |
| Example: | Router(config-if)# ip address 10.192.0.2 255.255.0.0 | |
| Step 5  | mpls ip | Enables MPLS. |
| Example: | Router(config-if)# mpls ip | |
| Step 6  | mpls label protocol ldp | Configures the mpls parameters. |
| Example: | Router(config-if)# mpls label protocol ldp | |
### Configuring Static MAC Binding to EVCs and Pseudowires

This section describes how to configure static MAC binding to EVCs and pseudowires.

#### SUMMARY STEPS

1. enable

### Configuring Static MAC over Pseudowire for the Cisco 7600 Router

This section describes how to configure static MAC over pseudowire.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# exit</td>
</tr>
<tr>
<td>Step 8</td>
<td>interface loopback loopback_Id</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface loopback 0</td>
</tr>
<tr>
<td>Step 9</td>
<td>ip address loopback_address mask</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# ip address 1.1.1.1 mask 255.255.255.255</td>
</tr>
<tr>
<td>Step 10</td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# exit</td>
</tr>
<tr>
<td>Step 11</td>
<td>mpls ldp router-id loopback loopback_Id force</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# mpls ldp router-id loopback 0 force</td>
</tr>
<tr>
<td>Step 12</td>
<td>router ospf ospf_Id</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# router ospf 50</td>
</tr>
<tr>
<td>Step 13</td>
<td>network loopback_network wildcard_mask area 0</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# network 192.168.1.1 255.255.255.255 area 0</td>
</tr>
<tr>
<td>Step 14</td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>
2. configure terminal
3. l2 vfi vfi_Id manual
4. vpn id vpn_id
5. bridge-domain bd_number vlan
6. neighbor ip_address encapsulation mpls
7. mac static address mac_address
8. exit
9. Interface vlan vlan_Id
10. xconnect vfi vfi_Id
11. no shutdown
12. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>En· -</td>
</tr>
<tr>
<td>Router# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 l2 vfi vfi_name manual</td>
<td>Creates a VFI and enters L2 VFI configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-vfi)# l2 vfi smac_vfi manual</td>
<td></td>
</tr>
<tr>
<td>Step 4 vpn id vpn_id</td>
<td>Configure the VPN Identifier.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-vfi)# vpn id 30</td>
<td></td>
</tr>
<tr>
<td>Step 5 bridge-domain bd_number vlan</td>
<td>Configures the bridge domain.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(vfi-config)# bridge-domain 40 vlan</td>
<td></td>
</tr>
<tr>
<td>Step 6 neighbor ip_address encapsulation mpls</td>
<td>Configures the remote peering router-id and tunnel encapsulation type.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(vfi-config)# neighbor 192.168.1.1 encapsulation mpls</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Static MAC Binding to EVCs and Pseudowires

**Chapter 4  Configuring Layer 1 and Layer 2 Features**

**Examples**

This example shows how to configure static MAC over pseudowire.

```plaintext
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 4/1/0
Router(config)# 12 vfi foo-core manual
Router(config-vfi)# vpn id 100
Router(config-vfi)# bridge-domain 10 vlan
Router(config-vfi)# neighbor 11.0.0.1 encapsulation mpls
Router(config-vfi-neighbor)# mac static address 0002.1122.0010 auto-learn
Router(config-vfi-neighbor)# mac static address 0002.1122.0011
Router(config-vfi-neighbor)# mac static address 0002.1122.0012 disable-snooping
Router(config-vfi-neighbor)# mac static address 0002.1122.0013 auto-learn
Router(config-vfi-neighbor)# mac static address 0002.1122.0014 disable-snooping
Router(config-vfi-neighbor)# interface vlan 10
Router(config-if)# xconnect vfi smac_v-fi
Router(config-if)# exit
Router(config)# exit
```

---

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 7    | `mac static address mac_address [auto-learn | disable-snooping]` | Configures the unicast and/or multicast static MAC address to the interface. MAC address is in hexadecimal format. Configuring the static mac address for service instance. The option:  
  - auto-learn is used for unicast static MAC address only. This option is not available for multicast static mac address.  
  - disable-snooping is used for multicast static MAC address. This option disables IGMP snooping on the multicast MAC address. |
| 8    | `exit` | Exits the VFI configuration mode. |
| 9    | `Interface vlan vlan_Id` | Creates an interface VLAN, where the VLAN Id should be same as the bd_number configured in step 5. |
| 10   | `xconnect vfi VFI_Id` | Binds the Ethernet or VLAN port to the L2 VFI. |
| 11   | `exit` | Exits the interface configuration mode. |

---

#### Examples

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>`mac static address mac_address [auto-learn</td>
<td>disable-snooping]`</td>
</tr>
<tr>
<td>8</td>
<td><code>exit</code></td>
<td>Exits the VFI configuration mode.</td>
</tr>
<tr>
<td>9</td>
<td><code>Interface vlan vlan_Id</code></td>
<td>Creates an interface VLAN, where the VLAN Id should be same as the bd_number configured in step 5.</td>
</tr>
<tr>
<td>10</td>
<td><code>xconnect vfi VFI_Id</code></td>
<td>Binds the Ethernet or VLAN port to the L2 VFI.</td>
</tr>
<tr>
<td>11</td>
<td><code>exit</code></td>
<td>Exits the interface configuration mode.</td>
</tr>
</tbody>
</table>
Verification

Use the following commands to verify a configuration:

- You can use the `show bridge-domain domain_Id mac static address` command to verify the configuration:

  Bridge-Domain ID : 10
  Static MAC count : System : 8, bridge-domain : 8
  Port Address Action
  vfi foo-core neighbor 1.1.1.1 100 0000.0200.1112
  vfi foo-core neighbor 1.1.1.1 100 0000.1111.1001 auto-learn
  vfi foo-core neighbor 1.1.1.1 100 0100.5e11.1002
  vfi foo-core neighbor 1.1.1.1 100 0100.5e11.1003 disable-snooping
  Gi2/0/0 ServInst 2 0000.1111.1003
  Gi2/0/0 ServInst 2 0000.1111.1004 auto-learn
  Po500 ServInst 1 0000.0000.0777
  Po500 ServInst 1 0100.5e00.1111 disable-snooping

- You can use the `show ethernet service instance id si_Id interface interface mac static address` command to verify the configuration:

  Router#Router# show ethernet service instance id 1 interface Gi 2/0/0 mac static address
  Bridge domain ID : 10
  Port static MAC count : 2
  Port Address Action
  Gi2/0/0 ServInst 1 0000.1111.1001
  Gi2/0/0 ServInst 1 0000.1111.1002 auto-learn

- You can use the `show vfi { name vfi_name> | neighbor peer_ip_address vcid id } mac static address` command to verify the configuration:

  Router#show vfi neighbor 1.1.1.1 vcid 100 mac static address
  Bridge domain ID : 10
  Port Address Action
  vfi foo-core neighbor 1.1.1.1 100 0000.0200.1112
  vfi foo-core neighbor 1.1.1.1 100 0000.1111.1001
  vfi foo-core neighbor 1.1.1.1 100 0000.1111.1002 auto-learn
  vfi foo-core neighbor 1.1.1.1 100 0100.5e11.1002

Troubleshooting

Table 4-27 provides the troubleshooting solutions for the REP over EVC feature
Configuring Resilient Ethernet Protocol

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to support L2 resiliency and fast failover with Ethernet networks. REP provides functionality to:

- Control network loops
- Handle link failures
- Improve convergence time

An REP segment is a connected chain of ports configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. REP is supported on Layer 2 trunk interfaces and EVC ports. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing. REP extends the network resiliency across Cisco IP Next-Generation Network (NGN) Carrier Ethernet Design. REP is designed to provide network and application convergence within 50 to 200 ms. REP is a segment protocol that integrates easily into existing Carrier Ethernet networks. It allows network architects to limit the scope of STP domains. REP can also notify the STP about potential topology changes, allowing interoperability with Spanning Tree.

REP is a distributed and secure protocol and does not rely on a master node controlling the status of the ring. Hence, the failures can be detected locally either through loss of signal (LOS) or loss of neighbor adjacency. Any REP port can initiate a switchover after acquiring the secure key to unblock the alternate port. An REP segment is a chain of ports connected to each other and configured with the same segment ID. Each end of a segment terminates on an edge switch. The port where the segment terminates is called the edge port.

---

**Table 4-27  Troubleshooting REP over EVC feature**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Pseudowire (PW) state changes | Complete these steps:  
1. If a PW is down, flush all the static MAC addresses configured within the PW.  
2. If the PW is up, re-install all the static MAC addresses configured within the PW.  
3. If there is a PW change in egress due to load-balancing or FRR, update all static MAC addresses configured within the PW in the HW MAC table to use the new egress information. |
| MAC address is not installed or deleted from the MAC address table  
Data is not synchronized with the standby supervisor  
EFP or PW is disabled | Use the `debug mac static [event | error | ha | issu]` command to confirm if the MAC address (configured through static mac over EFP/PW feature) is installed or deleted from the mac address table and if the data is synchronized to the standby supervisor. Share the output with TAC for further investigation. |
**REP Edge No-Neighbor**

Effective from Cisco IOS release 15.1.(01)S, a new functionality provides capability to configure the non-rep switch facing ports as edge no-neighbor ports. These ports inherit the properties of edge ports, and overcome the limitation of not being able to converge quickly during a failure.

![Figure 4-9 Edge No-Neighbor Ports](image)

In access ring topologies, the neighboring switch might not support REP, as shown in Figure 4-2. In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. These ports inherit all the properties of edge ports. You can configure these no-neighbor ports as any other edge port and also enable the ports to send STP or REP topology change notices to the aggregation switch. In this case the STP Topology Change Notice (TCN) that is sent is a Multiple Spanning-Tree (MST) STP message.

These sections describes how to configure REP on the Cisco 7600 router:

- Configuring REP over Ethernet Virtual Circuit, page 4-213
- Configuring Resilient Ethernet Protocol Configurable Timers, page 4-231

**Configuring REP over Ethernet Virtual Circuit**

The REP over Ethernet Virtual Circuit (EVC) allows you to configure and manage ports at service level. You cannot configure REP on per service instance. An EVC port can have multiple service instances. Each service instance corresponds to a unique Event Flow Processor (EFP). By default, REP is disabled on all ports. Using REP over EVC, you can:

- Control data traffic.
- Configure VLANs load balancing at service instance level.

The ports on a C7600 platform are classified into three different types: switchports, routed ports, and EVC ports. By default, a port is a routed port. REP is not supported on routed ports. You need to configure a port to a switchport or EVC port to configure REP on it. A port that is configured with one or more service instances is called an EVC port.
This feature allows you to configure an EVC port to participate in a REP segment. REP can selectively block or forward data traffic on particular VLANs. For EVC, the VLAN Id refers to the outer tag of the dot1q encapsulation that is configured on a service instance. REP is supported on a bridge-domain service. If `ethernet vlan color-block all` command is configured, REP is supported on connect and xconnect services.


### Restrictions and Usage Guidelines

When configuring REP over EVC for the Cisco 7600 router, follow these guidelines and restrictions:

- **REP is not supported on service instances configured with encapsulation, untagged, or default type.**
- **Cisco recommends that you begin by configuring one port and then configure the contiguous ports to minimize the number of segments and the number of blocked ports.**
- **REP can handle only one failure in a segment. If there is more than one failure in a REP segment, traffic is lost.**
- **REP ports must be Layer 2 trunk ports or EVC ports.**
- **You must configure all trunk ports in the segment with the same set of allowed VLANs, or a misconfiguration may occur.**
- **Since REP blocks all VLANs until another REP interface sends a message to unblock it, you might lose connectivity to the port if you enable REP in a Telnet session that accesses the EVC port through the same interface.**
- **You cannot execute REP and STP/MST or REP and Flex Links on the same segment or interface.**
- **If you connect an STP network to the REP segment, be sure that the connection is at the segment edge. An STP connection that is not at the edge causes a bridging loop because STP does not run on REP segments. All STP BPDUs are dropped at REP interfaces.**
- **If REP is enabled on two ports, both the ports must be either regular segment ports or edge ports. REP ports follow these rules:**
  - If only one port is configured in a segment, the port should be an edge port.
  - If two ports belong to the same segment, both ports must be edge ports or the regular segment ports.
  - If two ports belong to the same segment and one is configured as an edge port and other as a regular segment port, the edge port is treated as a regular segment port.
  - There can be only two edge ports in a segment, if there are two edge routers in a segment, each router can have only one edge port. All the other ports on the edge router function as normal ports.
- **REP interfaces come up in a blocked state and remains in a blocked state until notified that it is safe to unblock.**
- **REP sends all LSL PDUs in untagged frames on the native VLAN. The BPA message(untagged) sent to the Cisco multicast address is sent on the administration VLAN, which is VLAN 1 by default. Only the hardware flood layer (HFL) packets are sent on admin VLAN.**
- **REP ports cannot be configured as:**
- SPAN destination port
- Private VLAN port
- Tunnel port
- Access port

- REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel. It is supported on Switchports and EVC port-channels. REP is implemented on Port-channels instead of individual ports.

- In case of double VLAN tagged frame, REP is implemented only on the outer VLAN tag.

- When an edge no-neighbor is configured on a router, configuring and unconfiguring an edge port is not allowed.

- Starting with Cisco IOS Release 15.2(4)S, you can configure a maximum of two REP edge no-neighbor ports on the same segment.

- The Cisco 7600 Series Router supports 2000 VLANs when a scaled number of more than 8 REP segments are configured.

**Configuring REP over EVC for the Cisco 7600 Router**

This section describes how to configure REP over EVC for the Cisco 7600 router:

- Configuring REP over EVC using cross-connect on the Cisco 7600 Router, page 4-215
- Configuring REP over EVC using connect for the Cisco 7600 Router, page 4-219
- Configuring REP over EVC using bridge-domain for the Cisco 7600 Router, page 4-224

**Configuring REP over EVC using cross-connect on the Cisco 7600 Router**

This section describes how to configure REP over EVC using cross-connect at global configuration level.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface gigabitEthernet slot/port
4. rep segment segment_id [edge [no-neighbor] [primary]] [preferred]
5. ether vlan color-block all
6. service instance id {Ethernet [service-name]
7. encapsulation dot1q vlan_id
8. rewrite ingress tag [push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | symmetric]}
9. xconnect loopback_ip vc_id encapsulation mpls
10. exit
## Configuring Resilient Ethernet Protocol

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
- Enter your password if prompted.  

**Example:**  
Router# enable |

| **Step 2** | configure terminal | Enters global configuration mode.  

**Example:**  
Router# configure terminal |

| **Step 3** | interface gigabitethernet slot/port | Specifies the Gigabit Ethernet interface to configure, where:  
- slot/port—Specifies the location of the interface.  

**Example:**  
Router(config)# interface gigabitethernet 5/3 |
### Configuring Resilient Ethernet Protocol

#### Step 4

**Command**

`rep segment segment_id [edge [no-neighbor] [primary]] [preferred]`

**Example:**

```
Router(config-if)# rep segment 3 edge
```

- **Purpose**: Configures the REP over EVC. The segment ID range is from 1 to 1024.
- **Note**: You must configure two edge ports, including one primary edge port for each segment.

These optional keywords are available:

- **edge** to configure the port as an edge port. Entering `edge` without the `primary` keyword configures the port as the secondary edge port. Each segment has only two edge ports.
- **primary** to configure the port as the primary edge port, the port on which you can configure VLAN load balancing.
- **no-neighbor** to configure the segment edge with no external rep neighbor.
- **preferred** to indicate that the port is the preferred alternate port, or the preferred port for VLAN load balancing.

This **Note**: Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the `primary` keyword on both switches, the configuration is allowed. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by using the `show rep topology` privileged EXEC command.

- **Note**: Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

#### Step 5

**Command**

`ether vlan color-block all`

**Example:**

```
Router(config-if)# ether vlan color-block all
```

- **Purpose**: Configures REP to block xconnect type of service instances.

#### Step 6

**Command**

`service instance id Ethernet [service-name]`

**Example:**

```
Router(config-if)# service instance 101 ethernet
```

- **Purpose**: Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.
### Example

This example shows how to configure REP over EVC using xconnect.

```text
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 5/3
Router(config-if)# rep segment 120 edge
Router(config-if)# ether vlan color-block all
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# xconnect 10.0.0.1 20 encapsulation mpls
Router(config-if-ether-vc-xconn)# exit
Router(config-if-srv)# exit
Router(config-if)# exit
Router(config)# exit
```
Configuring REP over EVC using connect for the Cisco 7600 Router

This section describes how to configure REP over EVC using connect at global configuration level.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. ether vlan color-block all
5. service instance id {Ethernet [service-name]}
6. encapsulation dot1q vlan_id
7. rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-second-dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id} | 1-to-2 {dot1q vlan-second-dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id | dot1ad vlan-id} | 2-to-2 {dot1q vlan-id | dot1q vlan-second-dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id} [symmetric]}
8. exit
9. rep segment segment_id [edge [no-neighbor] [primary]] [preferred]
10. exit
11. interface type slot/port
12. ether vlan color-block all
13. service instance id {Ethernet [service-name]}
14. encapsulation dot1q vlan_id
15. rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-second-dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id} | 1-to-2 {dot1q vlan-second-dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id | dot1ad vlan-id} | 2-to-2 {dot1q vlan-id | dot1q vlan-second-dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id} [symmetric]}
16. exit
17. rep segment segment_id [edge [no-neighbor] [primary]] [preferred]
18. exit
19. connect <connect_name> <interface> <service_instance_id> <interface> <service_instance_id>
# Configuring Resilient Ethernet Protocol

## Chapter 4  Configuring Layer 1 and Layer 2 Features

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** | Router# enable |
| **Step 2** | configure terminal | Enters global configuration mode. |
| **Example:** | Router# configure terminal |
| **Step 3** | interface gigabitethernet slot/port | Specifies the Gigabit Ethernet interface to configure, where: 
*slot/port*—Specifies the location of the interface. |
| **Example:** | Router(config)# interface gigabitethernet 2/1 |
| **Step 4** | ether vlan color-block all | Configures REP to block connect type of service instances. |
| **Example:** | Router(config-if)# Ether vlan color-block all |
| **Step 5** | service instance id Ethernet [service-name] | Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode. |
| **Example:** | Router(config-if)# service instance 10 ethernet |
| **Step 6** | encapsulation dot1q {any | vlan-id[vlan-id[-vlan-id]]} second-dot1q {any | vlan-id[vlan-id[-vlan-id]]} | Configures the encapsulation. Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance. |
| **Example:** | Router(config-if-srv)# encapsulation dot1q 10 |
### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.</td>
</tr>
<tr>
<td>`rewrite ingress tag {push (dot1q vlan-id</td>
<td>dot1q vlan-id second-dot1q vlan-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if-srv)# rewrite ingress tag pop 1 symmetric</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Exits service instance mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if-srv)# exit</td>
</tr>
</tbody>
</table>
### Configuring Resilient Ethernet Protocol

**Step 9**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| rep segment segment_id [edge [no-neighbor] [primary]] [preferred] | Configures REP over EVC. The segment ID range is from 1 to 1024.  
**Note** You must configure two edge ports, including one primary edge port for each segment.  
These optional keywords are available.  
- Enter `edge` to configure the port as an edge port. Entering `edge` without the `primary` keyword configures the port as the secondary edge port. Each segment has only two edge ports.  
- On an edge port, enter `primary` to configure the port as the primary edge port, the port on which you can configure VLAN load balancing. **Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the `primary` keyword on both switches, the configuration is allowed. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by using the `show rep topology` privileged EXEC command.  
- On an edge port, use the `no-neighbor` keyword to configure the segment edge with no external rep neighbor.  
- Enter `preferred` to indicate that the port is the preferred alternate port, or the preferred port for VLAN load balancing. Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port. |
| Example: Router(config-if)# rep segment 2 edge primary |

**Step 10**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Step 11**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| interface gigabitethernet slot/port | Specifies the Gigabit Ethernet interface to configure, where:  
`slot/port`—Specifies the location of the interface. |
| Example: Router(config)# interface gigabitethernet 3/1 |
### Command

#### Step 12
```
ether vlan color-block all
```

**Example:**
```
Router(config-if)# Ether vlan color-block all
```

- **Purpose:** Configures REP to block connect type of service instances.

#### Step 13
```
service instance id Ethernet [service-name]
```

**Example:**
```
Router(config-if)# service instance 102 ethernet
```

- **Purpose:** Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.

#### Step 14
```
encapsulation dot1q (any | vlan-id[vlan-id]) second-dot1q (any | vlan-id[vlan-id])
```

**Example:**
```
Router(config-if-srv)# encapsulation dot1q 100 second dot1q 200
```

- **Purpose:** Configures the encapsulation. Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.

#### Step 15
```
rewrite ingress tag (push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 | 2-to-1 dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id}) [symmetric] tag pop id symmetric
```

**Example:**
```
Router(config-if-srv)# rewrite ingress tag push dot1q 20
```

- **Purpose:** Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.

#### Step 16
```
exit
```

**Example:**
```
Router(config-if-srv)# exit
```

- **Purpose:** Exits service instance mode.

#### Step 17
```
rep segment segment_id [edge [no-neighbor] [primary]] [preferred]
```

**Example:**
```
Router(config-if)# rep segment 2 edge primary
```

- **Purpose:** Configures REP over EVC.
Chapter 4      Configuring Layer 1 and Layer 2 Features

Configuring Resilient Ethernet Protocol

### Command

<table>
<thead>
<tr>
<th>Step 18</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Exits interface configuration mode.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step 19</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>connect &lt;connect_name&gt; &lt;interface&gt; &lt;service_instance_id&gt; &lt;interface&gt; &lt;service_instance_id&gt;</td>
<td>Configures local connect between the two service instances of two different interfaces.</td>
</tr>
</tbody>
</table>

Example:
```
outer(config)#connect test gigabitEthernet 2/1 10 gigabitEthernet 3/1 20
```

### Examples

This example shows how to configure REP over EVC using connect.
```
Router# enable
Router# configure terminal
Router(config)# interface gigabitEthernet 2/1
Router(config-if)# ether vlan color-block all
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# exit
Router(config-if)# rep segment 2 edge primary
Router(config-if)# exit
Router(config)# interface gigabitEthernet 3/1
Router(config-if)# service instance 20 ethernet
Router(config-if-srv)# encapsulation dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# exit
Router(config-if)# rep segment 2 edge
Router(config-if)# exit
Router(config)# connect test gigabitEthernet 2/1 10 gigabitEthernet 3/1 20
Router(config-connection)#end
```

### Configuring REP over EVC using bridge-domain for the Cisco 7600 Router

This section describes how to configure REP over EVC using bridge-domain at service instance level.

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. service instance id {Ethernet [service-name]}
5. encapsulation dot1q vlan_id
6. rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id}}
   [symmetric]

7. bridge-domain bd_Id

8. exit

9. rep segment segment_id [edge [no-neighbor] [primary]] [preferred]

10. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface gigabitethernet slot/port</td>
<td>Specifies the Gigabit Ethernet interface to configure, where: slot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface gigabitethernet 4/1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>service instance id Ethernet [service-name]</td>
<td>Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-srv)# service instance 101 ethernet</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>encapsulation dot1q (any</td>
<td>Configures the encapsulation. Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td>vlan-id[vlan-id[-vlan-id]]} second-dot1q (any</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-id[vlan-id[-vlan-id]])</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-srv)# encapsulation dot1q 100 second dot1q 200</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Resilient Ethernet Protocol

#### Step 6
Rewrite ingress tag:

```
rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 {dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} [symmetric]}
```

**Example:**

```
Router(config-if-srv)# rewrite ingress tag push dot1q 20
```

**Purpose:** Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.

#### Step 7
Bridge-domain:

```
bridge-domain bd_Id
```

**Example:**

```
Router(config-if-srv)# bridge-domain 10
```

**Purpose:** Configures bridge-domain to add another VLAN tag of type bridge-domain to the incoming packet.

#### Step 8
Exit:

```
exit
```

**Example:**

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

**Purpose:** Exits service instance mode.
### Command

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 9    | rep segment segment_id [edge [no-neighbor] [primary]] [preferred] | Configures REP over EVC. The segment ID range is from 1 to 1024.  
**Note** You must configure two edge ports, including one primary edge port for each segment.  
These optional keywords are available.  
- Enter `edge` to configure the port as an edge port.  
  Entering `edge` without the `primary` keyword configures the port as the secondary edge port. Each segment has only two edge ports.  
- On an edge port, enter `primary` to configure the port as the primary edge port, the port on which you can configure VLAN load balancing.  
**Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the `primary` keyword on both switches, the configuration is allowed. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by using the `show rep topology` privileged EXEC command.  
- On an edge port, use the `no-neighbor` keyword to configure the segment edge with no external rep neighbor.  
- Enter `preferred` to indicate that the port is the preferred alternate port, or the preferred port for VLAN load balancing.  
Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port. |
| 10   | exit    | Exits global configuration mode. |

### Examples

This example shows how to configure REP over EVC using bridge-domain.

```
Router# enable  
Router# configure terminal  
Router(config)# interface gigabitEthernet 4/1  
Router(config-if)# service instance 10 ethernet  
Router(config-if-srv)# encapsulation dot1q 10  
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
```
This example shows how to configure REP with the edge `no-neighbor` keyword.

```
Router# enable
Router# configure terminal
Router(config)# interface gigabitEthernet 7/1
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# rep segment 1 edge no-neighbor primary
Router(config-if)# end
```

**Verification**

You can use the `show rep topology`, `show rep topology detail` and `show interface <> rep` commands to verify the REP over EVC configuration. This information is displayed as sample output:

- Specific EVCs if an EVC ID is specified.
- All the EVCs on an interface if an interface is specified.
- The detailed option provides additional information about the EVC. This can be given on RP and LC consoles to determine custom ethertype configured under a physical port.

**Example of `show rep topology` command:**

```
Router#show rep topology
REP Segment 3
BridgeName PortName Edge Role
-------------------------- ------ ---- ----
Router Gi4/0/0 Pri Open
REP-ALPHA Gi2/12 Open
REP-ALPHA Fa3/1 Open
REP-BETA Fa1/1 Open
REP-BETA G16/1 Open
Router Gi3/4 Sec Alt
```

**Example of `show rep topology detail` command.**

```
Router#show rep topology segment 3 detail
REP Segment 3
Router, Gi4/0/0 (Primary Edge)
Open Port, all vlans forwarding
Bridge MAC: 0015.fa66.ff80
Port Number: 0301
Port Priority: 000
Neighbor Number: 1 / [-6]
REP-ALPHA, Gi2/12 (Intermediate)
Open Port, all vlans forwarding
Bridge MAC: 0005.7495.cd00
Port Number: 010C
Port Priority: 000
Neighbor Number: 2 / [-5]
REP-ALPHA, Fa3/1 (Intermediate)
Open Port, all vlans forwarding
Bridge MAC: 0005.7495.cd00
Port Number: 0201
Port Priority: 000
Neighbor Number: 3 / [-4]
REP-BETA, Fa1/1 (Intermediate)
Open Port, all vlans forwarding
```
Bridge MAC: 0005.7495.c900
Port Number: 001
Port Priority: 000
Neighbor Number: 4 / 3
REP-BETA, Gi6/1 (Intermediate)
Open Port, all vlans forwarding
Bridge MAC: 0005.7495.c900
Port Number: 0501
Port Priority: 000
Neighbor Number: 5 / 2
Router, Gi3/4 (Secondary Edge)
Alternate Port, some vlans blocked
Bridge MAC: 0015.fA66.ff80
Port Number: 0204
Port Priority: 010
Neighbor Number: 6 / 1

Example of `show interface <> rep` command:
```
Router#show interface gig4/0/0 rep detail
GigabitEthernet4/0/0 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF800450
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

Show outputs for REP with Edge No-Neighbor keyword

Example of `show rep topology` command with REP edge `no-neighbor` keyword:
```
Router#show rep topology
REP Segment 3
BridgeName       PortName   Edge  Role
---------------- ---------- ----  ----
sw8-ts8-51       G10/2      Pri*  Open
sw9-ts11-50      G11/0/4    Open
sw9-ts11-50      G11/0/2    Open
sw1-ts11-45      G10/2      Alt
sw1-ts11-45      Po1        Open
sw8-ts8-51       G10/1      Sec* Open
```

Example of `show rep topology detail` command with REP edge `no-neighbor` keyword:
```
Router#show rep topology segment 3 detail
REP Segment 3
Router, Gi4/0/0 (Primary Edge No-Neighbor)
Open Port, all vlans forwarding
Configuring Resilient Ethernet Protocol

Chapter 4  Configuring Layer 1 and Layer 2 Features

Example of show interface <> rep command with REP edge no-neighbor keyword:

Router#show interface gig4/0/0 rep detail
GigabitEthernet4/0/0 REP enabled
Segment-id: 3 (Primary Edge No-Neighbor)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
Configuring Resilient Ethernet Protocol Configurable Timers

The REP Configurable Timer (REP Fast Hellos) feature provides a fast re-convergence in a ring topology with higher timer granularity and quicker failure detection on the remote side. The feature also supports improved convergence of REP segments having nodes with copper based SFPs, where the link detection time varies between 300 ms to 700 ms.

With the REP Link Status Layer (LSL) ageout timer configuration, the failure detection time can be configured between a range of 120 millisecond to 10,000 millisecond, in multiples of 40 ms. The result of this configuration is that, even if the copper pull takes about 700 ms to notify the remote end about the failure, the REP Configurable Timers process will detect it much earlier and takes subsequent action for the failure recovery within 200 ms.

Restrictions and Usage Guidelines

When configuring the REP Configurable Timers for the Cisco 7600 router, follow these guidelines and restrictions:

- The LSL Age Out Timer configuration is available on switchports, EVC, L2 Port-channel and Port-channel EVC interfaces.
- The SUP 720, RSP 720, RSP 10G supervisors and the ES20, ES40, and LAN line cards support the REP Configurable Timers configuration.
- While configuring REP configurable timers, we recommend you shut the port, configure REP and only then use the no shut command. This prevents the REP from flapping and generating large number of internal messages.
- If incompatible switches are neighbors, configure the correct LSL Age Out value first. In some scenarios, you might not get the expected convergence range.
- In order to inter-operate with switches running old IOS versions, the default LSL Age Out time is set to 5 seconds, default LSL retries is 5, and the hello packet is sent every one second.
- Except for the LSL Age Out time, all the other timer values are retained. For example, the EPA (End Port Advertisement) hello timer continues to be 4 seconds, as it is not required to send EPA PDUs at a higher frequency.
- While configuring REP configurable timers, we recommend you configure the REP LSL number of retries first and then configure the REP LSL age out timer value.
- Effective from Cisco IOS release 15.1(2)S:
  - The REP Configurable Timers feature is SSO compliant for RSP720, RSP10G (endor) and SUP720 supervisors.
  - The REP Configurable Timers feature on SSO is not supported with SUP32 supervisor.
  - The REP LSL Age Out value can be configured as low as 1520 ms (approximately 500 ms * 3) for HA systems as this prevents traffic loss.
  - The REP Configurable Timers feature is supported only on Cisco 7600 S-chassis.

Configuring REP Configurable Timers for the Cisco 7600 Router

This section describes how to configure the LSL age out timer and the LSL number of retries on a Cisco 7600 router:
Configuring the REP Link Status Layer Retries

This section describes how to configure REP link status layer number of retries at interface configuration level.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. rep segment segment_id [edge [no-neighbor] [primary]] [preferred]
5. rep lsl-retries <no-of-retries>
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enab[le</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router# enable</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>interface type slot/port</td>
<td>Specifies the Gigabit Ethernet, Ten Gigabit</td>
</tr>
<tr>
<td>Example:</td>
<td>Ethernet and Port Channel interfaces to</td>
</tr>
<tr>
<td>Router(config)# interface</td>
<td>configure, where:</td>
</tr>
<tr>
<td>gigabitethernet 2/5</td>
<td>• slot/port—Specifies the location of the</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
</tbody>
</table>
### Configuring Resilient Ethernet Protocol

#### Step 4

**Command**

```bash
rep segment segment_id [edge [no-neighbor] [primary]] [preferred]
```

**Example:**

```
Router(config-if)# rep segment 2 edge primary
```

**Purpose**

Configures the REP. The segment ID range is from 1 to 1024.

**Note**

You must configure two edge ports, including one primary edge port for each segment.

These optional keywords are available.

- Enter `edge` to configure the port as an edge port. Entering `edge` without the `primary` keyword configures the port as the secondary edge port. Each segment has only two edge ports.
- On an edge port, enter `primary` to configure the port as the primary edge port, the port on which you can configure VLAN load balancing.

**Note**

Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the `primary` keyword on both switches, the configuration is allowed. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by using the `show rep topology` privileged EXEC command.

- On an edge port, use the `no-neighbor` keyword to configure the segment edge with no external rep neighbor.
- Enter `preferred` to indicate that the port is the preferred alternate port or the preferred port for VLAN load balancing.

Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

#### Step 5

**Command**

```bash
rep lsl-retries <no-of-retries>
```

**Example:**

```
Router(config-if)# rep lsl-retries 4
```

**Purpose**

Configures the number of retries before the REP link is disabled. The acceptable range of retries is 3-10. The default LSL number of retries is 5.

#### Step 6

**Command**

```bash
end
```

**Example:**

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

**Purpose**

Exits configuration mode.

### Example

This example shows how to configure REP link status layer number of retries.

```
Router# enable
Router# configure terminal
Router(config)# interface gigabitethernet 2/5
```
Configuring Resilient Ethernet Protocol

Configuring the REP Link Status Layer Age Out Timer

This section describes how to configure the REP Link Status Layer Age Out Timer at interface configuration level.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. rep segment segment_id [edge [no-neighbor] [primary]] [preferred]
5. rep lsl-age-timer <lsl-age-timer>
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router# enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type slot/port</td>
<td>Specifies the Gigabit Ethernet, Ten Gigabit Ethernet and Port Channel interfaces to configure, where:</td>
</tr>
<tr>
<td>Example: Router(config)# interface gigabitethernet 5/3</td>
<td>• slot/port—Specifies the location of the interface.</td>
</tr>
</tbody>
</table>
### Configuring Resilient Ethernet Protocol

**Step 4**

```
rep segment segment_id [edge [no-neighbor] [primary]] [preferred]
```

**Example:**

Router(config-if)# rep segment 1 edge primary

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the REP. The segment ID range is from 1 to 1024.</td>
</tr>
<tr>
<td><code>rep segment segment_id [edge [no-neighbor] [primary]] [preferred]</code></td>
<td><strong>Note</strong> You must configure two edge ports, including one primary edge port for each segment.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>These optional keywords are available.</td>
</tr>
<tr>
<td>Router(config-if)# rep segment 1 edge primary</td>
<td>• Enter <code>edge</code> to configure the port as an edge port. Entering <code>edge</code> without the <code>primary</code> keyword configures the port as the secondary edge port. Each segment has only two edge ports.</td>
</tr>
<tr>
<td></td>
<td>• On an edge port, enter <code>primary</code> to configure the port as the primary edge port, the port on which you can configure VLAN load balancing.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the <code>primary</code> keyword on both switches, the configuration is allowed. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by using the <code>show rep topology</code> privileged EXEC command.</td>
</tr>
<tr>
<td></td>
<td>• On an edge port, use the <code>no-neighbor</code> keyword to configure the segment edge with no external rep neighbor.</td>
</tr>
<tr>
<td></td>
<td>• Enter <code>preferred</code> to indicate that the port is the preferred alternate port, or the preferred port for VLAN load balancing.</td>
</tr>
</tbody>
</table>

**Step 5**

```
rep lsl-age-timer <lsl-age-timer>
```

**Example:**

Router(config-if)# rep lsl-age-timer 2000

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures REP link status layer age out timer value. The acceptable range of lsl-age-timer is between 120ms and 10000ms, in multiples of 40ms. The default LSL Age Out time is 5 seconds.</td>
</tr>
<tr>
<td><code>rep lsl-age-timer &lt;lsl-age-timer&gt;</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# rep lsl-age-timer 2000</td>
<td></td>
</tr>
</tbody>
</table>

**Step 6**

```
end
```

**Example:**

Router(config-if)# end

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4 Configuring Layer 1 and Layer 2 Features

Configuring Resilient Ethernet Protocol

Router(config)# interface GigabitEthernet 5/3
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep lsl-age-timer 2000
Router(config-if)# end

Verification

Use the show interfaces <interface name> rep detail command to view the configured LSL number of retries and the LSL Age Out timer values.

7600-1#show interfaces GigabitEthernet11/1 rep detail
 GigabitEthernet11/1   REP enabled
    Segment-id: 10 (Segment)
    PortID: 0A010009B6D8F700
    Preferred flag: No
    Operational Link Status: NO_NEIGHBOR
    Current Key: 0A010009B6D8F700EEA1
    Port Role: Fail No Ext Neighbor
    Blocked VLAN: 1-4094
    Admin-vlan: 1
    Preempt Delay Timer: disabled
    LSL Ageout Timer: 120 ms
    LSL Ageout Retries: 3
    Configured Load-balancing Block Port: none
    Configured Load-balancing Block VLAN: none
    STCN Propagate to: none
    LSL PDU rx: 0, tx: 175
    HFL PDU rx: 0, tx: 0
    BPA TLV rx: 0, tx: 0
    BPA (STCN, LSL) TLV rx: 0, tx: 0
    BPA (STCN, HFL) TLV rx: 0, tx: 0
    EPA-ELECTION TLV rx: 0, tx: 0
    EPA-COMMAND TLV rx: 0, tx: 0
    EPA-INFO TLV rx: 0, tx: 0

Troubleshooting the REP

Table 4-28 lists the debug commands to troubleshoot the REP issues.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug rep bpa-event</td>
<td>Provides information about the BPA (Block Port Advertisement) events.</td>
</tr>
<tr>
<td>debug rep bpasm</td>
<td>Provides information about the BPA state machine.</td>
</tr>
<tr>
<td>debug rep chkpt</td>
<td>Provides information about the checkpoint events.</td>
</tr>
<tr>
<td>debug rep database</td>
<td>Provides information about the protocol database.</td>
</tr>
<tr>
<td>debug rep em</td>
<td>Provides information about the event manager events.</td>
</tr>
<tr>
<td>debug rep epasm</td>
<td>Provides information about the EPA (End Port Advertisement) state machine.</td>
</tr>
<tr>
<td>debug rep error</td>
<td>Provides information about the REP error thrown.</td>
</tr>
</tbody>
</table>
IEEE 802.1ag-2007 Compliant CFM

A Metro Ethernet network consists of networks from multiple operators supported by one service provider and connects multiple customer sites to form a virtual private network (VPN). Networks provided and managed by multiple independent service providers have restricted access to each other's equipment. Because of the diversity in these multiple-operator networks, failures must be isolated quickly. As a Layer 2 network, Ethernet must be capable of reporting network faults at Layer 2.
IEEE 802.3ah is a point-to-point and per-physical-wire OAM protocol that detects and isolates connectivity failures in the network. IEEE 802.1ag draft 8.1 *Metro Ethernet Connectivity Fault Management (CFM)* incorporates several OAM facilities that allow you to manage Metro Ethernet networks, including an Ethernet continuity check, end-to-end Ethernet traceroute facility using Linktrace message (LTM), Linktrace reply (LTR), Ethernet ping facility using Loopback Message (LBM), and a Loopback Reply (LBR). These Metro Ethernet CFM protocol elements quickly identify problems in the network.

Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs. Connectivity Fault Management (CFM) is the indispensable capability that service providers require to deploy large-scale, multivendor Metro Ethernet services. This feature upgrades the implementation of CFM to be compliant with the IEEE 802.1ag with the current standard, 802.1ag-2007 and implementation of CFM over L2VFI (Layer 2 Virtual Forwarding Instance Information), cross connect, EVC, and Switchport.

Key CFM mechanisms are:

- Maintenance domains (MDs) that break up the responsibilities for the network administration of a given end-to-end service.
- Maintenance associations (MAs) that monitor service instances within a specified MD.
- Maintenance points, (MPs or MIPs), such as Maintenance end points (MEP's) that transmit and receive CFM protocol messages, and MIPs that catalog information received from MEPs, and respond to Linktrace and Loopback messages.
- Protocols (Continuity Check, Loopback, and Linktrace) that are used to manage faults.


### Supported Line Cards

Use the `ethernet cfm global` command to enable the CFM D8.1 feature on the following line cards:

- ES20 and ES40: Switchports, routed ports, and EVC BD.
- SIP400: Routed ports, and Layer 2 Virtual Forwarding Instance (L2VFI).
- SIP600: Switchports, and routed ports.
- 67xx: Switchports, and routed ports.

Table 4-30 and Table 4-31 display the complete support matrix for the CFM D8.1 feature.

---

**Note**

The matrix is spread over two tables for better readability.
### Table 4-30  Supported Matrix1

<table>
<thead>
<tr>
<th>Line card</th>
<th>CFM on Switchport or CFM on Switch + BD for SVI Based EoMPLS for VPLS (pre-std)</th>
<th>CFM on Routed Port (pre-std)</th>
<th>CFM on Service Instance with BD for SVI based EoMPLS for VPLS (pre-std)</th>
<th>CFM on Switchport or CFM on Switch + BD (Standard)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SUP720-3BXL</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
<tr>
<td>WS-SUP720-3B</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
<tr>
<td>RSP720-3CXL-10GE</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
<tr>
<td>RSP720-3C-10GE</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
<tr>
<td>RSP720-3CXL-GE</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
<tr>
<td>RSP720-3C-GE</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
<tr>
<td>WS-SUP32-GE-3B</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
<tr>
<td>WS-SUP32-10GE-3B</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
<tr>
<td>WS-X6148A</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
</tbody>
</table>
## IEEE 802.1ag-2007 Compliant CFM

### Chapter 4 Configuring Layer 1 and Layer 2 Features

<table>
<thead>
<tr>
<th>Line card</th>
<th>CFM on Switchport or CFM on Switch + BD for SVI Based EoMPLS for VPLS (pre-std)</th>
<th>CFM on Routed Port (pre-std)</th>
<th>CFM on Service Instance with BD for SVI based EoMPLS for VPLS (pre-std)</th>
<th>CFM on Switchport or CFM on Switch + BD (Standard)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-X6148-FE-SFP</td>
<td>Up MEP</td>
<td>Down MEP Port MEP</td>
<td>Not Applicable</td>
<td>Up MEP Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6516A-GBIC</td>
<td>Up MEP</td>
<td>Down MEP Port MEP</td>
<td>Not Applicable</td>
<td>Up MEP Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6524-100FX-MM</td>
<td>Up MEP</td>
<td>Down MEP Port MEP</td>
<td>Not Applicable</td>
<td>Up MEP Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6548-RJ-21</td>
<td>Up MEP</td>
<td>Down MEP Port MEP</td>
<td>Not Applicable</td>
<td>Up MEP Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6548-GE-TX</td>
<td>Up MEP</td>
<td>Down MEP Port MEP</td>
<td>Not Applicable</td>
<td>Up MEP Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6704-10GE</td>
<td>Up MEP</td>
<td>Down MEP Port MEP</td>
<td>Not Applicable</td>
<td>Up MEP Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6708-10G-3C</td>
<td>Up MEP</td>
<td>Down MEP Port MEP</td>
<td>Not Applicable</td>
<td>Up MEP Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6708-10G-3CX L</td>
<td>Up MEP</td>
<td>Down MEP Port MEP</td>
<td>Not Applicable</td>
<td>Up MEP Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6724-SFP</td>
<td>Up MEP</td>
<td>Down MEP Port MEP</td>
<td>Not Applicable</td>
<td>Up MEP Down MEP Port MEP</td>
</tr>
</tbody>
</table>
### Chapter 4      Configuring Layer 1 and Layer 2 Features

IEEE 802.1ag-2007 Compliant CFM

<table>
<thead>
<tr>
<th>Line card</th>
<th>CFM on Switchport or CFM on Switch + BD for SVI Based EoMPLS for VPLS (pre-std)</th>
<th>CFM on Routed Port (pre-std)</th>
<th>CFM on Service Instance with BD for SVI based EoMPLS for VPLS (pre-std)</th>
<th>CFM on Switchport or CFM on Switch + BD (Standard)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-X6748-GE-TX</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
<tr>
<td>WS-X6748-SFP</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Applicable</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
<tr>
<td>SIP-400 + V2 GE SPAs or SIP-400 + WAN SPA</td>
<td>Not Supported ( SIP-400 + WAN SPA or SIP-400 + v2 GE SPA as uplink) No Transparency with CFM Enabled on the box</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td></td>
<td>Not Supported</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP-400 + V2 FE SPA or SIP-400 + WAN SPA</td>
<td>Not Supported ( SIP-400 + WAN SPA or SIP-400 + V2 GE SPA as uplink No Transparency with CFM Enabled on the box</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td></td>
<td>Not Supported</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP-600 + V2 GE or v2 10GE SPA or WAN SPA</td>
<td>Up MEP</td>
<td>Down MEP</td>
<td>Not Supported</td>
<td>Up MEP</td>
</tr>
<tr>
<td></td>
<td>Down MEP</td>
<td>Port MEP</td>
<td></td>
<td>Down MEP</td>
</tr>
<tr>
<td></td>
<td>Port MEP</td>
<td></td>
<td></td>
<td>Port MEP</td>
</tr>
</tbody>
</table>
### Table 4-31 Supported Matrix 2

<table>
<thead>
<tr>
<th>Line card</th>
<th>CFM on Switchport or CFM on Switch + BD for SVI Based EoMPLS for VPLS (pre-std)</th>
<th>CFM on Service Instance with BD for SVI based EoMPLS for VPLS (pre-std)</th>
<th>CFM on Switchport or CFM on Switch + BD (Standard)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES20-GE or ES20-10GE</td>
<td>Up MEP&lt;br&gt;Down MEP&lt;br&gt;Port MEP</td>
<td>Down MEP&lt;br&gt;Port MEP</td>
<td>Up MEP&lt;br&gt;Down MEP&lt;br&gt;Port MEP</td>
</tr>
<tr>
<td>ES+ GE /10GE</td>
<td>Up MEP&lt;br&gt;Down MEP&lt;br&gt;Port MEP</td>
<td>Down MEP&lt;br&gt;Port MEP</td>
<td>Up MEP&lt;br&gt;Down MEP&lt;br&gt;Port MEP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Line card</th>
<th>CFM on Service Instance + xconnect (Standard)</th>
<th>CFM on Service Instance + BD for SVI based EoMPLS for VPLS (Standard)</th>
<th>CFM on L2-VFI (Standard)</th>
<th>CFM on Routed Port (Standard)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SUP720-3BXL</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP&lt;br&gt;Port MEP</td>
</tr>
<tr>
<td>WS-SUP720-3B</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP&lt;br&gt;Port MEP</td>
</tr>
<tr>
<td>RSP720-3CXL-10GE</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP&lt;br&gt;Port MEP</td>
</tr>
<tr>
<td>RSP720-3C-10GE</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP&lt;br&gt;Port MEP</td>
</tr>
<tr>
<td>RSP720-3CXL-GE</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP&lt;br&gt;Port MEP</td>
</tr>
</tbody>
</table>
### IEEE 802.1ag-2007 Compliant CFM

<table>
<thead>
<tr>
<th>Line card</th>
<th>CFM on Service Instance + xconnect (Standard)</th>
<th>CFM on Service Instance + BD for SVI based EoMPLS for VPLS (Standard)</th>
<th>CFM on L2-VFI (Standard)</th>
<th>CFM on Routed Port (Standard)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSP720-3C-GE</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-SUP32-GE-3B</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-SUP32-10GE-3B</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6148A</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6148-FE-SFP</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6516A-GBIC</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6524-100FX-MM</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6548-RJ-21</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6548-GE-TX</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6704-10GE</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>Line card</td>
<td>CFM on Service Instance + xconnect (Standard)</td>
<td>CFM on Service Instance + BD for SVI based EoMPLS for VPLS (Standard)</td>
<td>CFM on L2-VFI (Standard)</td>
<td>CFM on Routed Port (Standard)</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>WS-X6708-10G-3C</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6708-10G-3CX L</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6724-SFP</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6748-GE-TX</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>WS-X6748-SFP</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>SIP-400 + V2 GE SPAs or SIP-400 + WAN SPA</td>
<td>Not Supported No Transparency</td>
<td>Not Supported No Transparency</td>
<td>Down MEP</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>SIP-400 + V2 FE SPA or SIP-400 + WAN SPA</td>
<td>Not Supported No Transparency</td>
<td>Not Supported No Transparency</td>
<td>Down MEP</td>
<td>Down MEP Port MEP</td>
</tr>
<tr>
<td>SIP-600 + V2 GE or V2 10GE SPA or WAN SPA</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Down MEP</td>
<td>Down MEP Port MEP</td>
</tr>
</tbody>
</table>
## Scalable Limits

Table 4-32 maps the supported interfaces with the CFM points and their scalability values.

<table>
<thead>
<tr>
<th>Interfaces</th>
<th>CFM Points</th>
<th>Scalability Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switchports and EVC Bridge Domain (BD)</td>
<td>Up MEP, Down MEP, MIP, Port MEP</td>
<td>8K MEPs per box (4K MEPs per LC) at 10 sec CC interval or higher CC intervals. 1K MEPs at 1 sec CC interval or higher CC intervals. 100 MEPs at 100 msec CC interval or higher CC intervals.</td>
</tr>
<tr>
<td>Routed Ports</td>
<td>Down MEP, Port MEP</td>
<td>1K MEPs at 1 sec CC interval or higher CC intervals. 100 MEPs at 100 msec CC interval or higher CC intervals. 4K MEPs per box at 10 sec CC interval or higher CC intervals.</td>
</tr>
<tr>
<td>L2-VFI</td>
<td>Down MEP</td>
<td>1K MEPs at 10 sec CC interval or higher CC intervals.</td>
</tr>
</tbody>
</table>

## Restrictions and Usage Guidelines

When configuring CFM D8.1, follow these restrictions and usage guidelines:

- Hardware EoMPLS is not supported.
- Supports interworking between routed ports, switch ports, and EVC BD.
- CFM D8.1 QinQ configuration on a subinterface is not supported.
- You can ping or traceroute to a MEP where Continuity Check (CC) is disabled. However, you cannot use ping and traceroute for an down MEP on a STP blocked port configured on either a supervisor port or a LAN port.
- With lower CC intervals, CC packets are transmitted in bursts. Ensure that you appropriately configure the MLS rate limiters to avoid flapping of remote MEPs.
- Ping and traceroute on trunk ports for Port-MEP's and down MEP's configured on native vlan is supported only on ES20 and ES40 line cards.
- In 802.3ah E-OAM, the remote-loopback TEST status is not retained across switchovers. The remote loopback works with a longer OAM timeout value that is greater than 10 seconds.
- CFM is not supported with a EVC manual load balancing configuration on a EVC bridge-domain and a EVC cross-connect interface. Though configuration is not rejected, the feature may not work as expected.
- Migrating CFM D1.0 to D8.1 works with a reduced scale of 2k MEPs on the routed ports. For example, if there is an EVC service configured within a domain in D1, the link fails while migrating to D8.1. To avoid this, ensure that you configure the VLAN and the EVC within the domain in D1, as shown in the next example.

Sample D1 configuration during migration:
```
ethernet cfm domain 2OUT493 level 2 direction outward
service 1 evc 493
```
Sample configuration to avoid the migration issue:
```
ethernet cfm domain 2OUT493 level 2 direction outward
service 1 evc 493
service 1 vlan 493
```

**SUMMARY STEPS (COMMON CONFIGURATIONS FOR EVC, SWITCHPORT, AND ROUTED PORTS)**

1. `enable`
2. `configure terminal`
3. `ethernet cfm domain domain-name level level-id`
4. `service { short-ma-name | number MA-number | vlan-id primary-vlan-id | vpn-id vpn-id } {vlan vlan-id | port | evc evc-name }`
5. `continuity-check`
6. `continuity-check {interval CC-interval }`
7. `end`
### DETAILED STEPS (COMMON CONFIGURATIONS FOR EVC, SWITCHPORT, AND ROUTED PORTS)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | `enable` | Enables privileged EXEC mode.  
*Example:*  
Router> enable  
*Purpose:* Enter your password if prompted. |
| 2    | `configure terminal` | Enters global configuration mode. |
| 3    | `ethernet cfm domain domain-name level level-id` | Defines a CFM maintenance domain at a particular maintenance Level. It sets the router into config-ecfm configuration mode, where parameters specific to the maintenance domain can be set.  
*Example:*  
PE1(config)#ethernet cfm domain L4 level 4 |
| 4    | `service { short-ma-name | number | vlan-id primary-vlan-id | vpn-id vpn-id }` | Configures the maintenance association and sets a universally unique ID for a customer service instance (CSI) or the maintenance association number value, primary VLAN ID and VPN ID within a maintenance domain in Ethernet connectivity fault management (CFM) configuration mode.  
*Example:*  
Router(config-ecfm)#service s41 evc 41 vlan 41 |
| 5    | `continuity-check` | Configures the transmission of continuity check messages (CCMs), in Ethernet connectivity fault management (CFM) service configuration mode.  
*Example:*  
Router(config-ecfm-srv)#continuity-check |
IEEE 802.1ag-2007 Compliant CFM

SUMMARY STEPS TO CONFIGURE CFM MEP AND MIP ON A EVC

1. enable
2. configure terminal
3. interface
4. service instance \{id\} ethernet \{evc-name\}
5. encapsulation \{encapsulation-type\}
6. bridge-domain \{number\}
7. cfm mep domain \{domain-name\} mpid \{id\}
8. cfm mip level \{level\}
9. cfm encapsulation
10. end

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6 continuity-check (interval CC-interval )</td>
<td>Configures the per-service parameters and sets the interval at which Continuity Check Messages are transmitted.</td>
</tr>
<tr>
<td>Example: Router(config-ecfm-srv)#continuity-check interval 10s</td>
<td>• The supported interval values are:</td>
</tr>
<tr>
<td></td>
<td>- 100ms 100 ms</td>
</tr>
<tr>
<td></td>
<td>- 10m 10 minutes</td>
</tr>
<tr>
<td></td>
<td>- 10ms 10 ms</td>
</tr>
<tr>
<td></td>
<td>- 10s 10 seconds</td>
</tr>
<tr>
<td></td>
<td>- 1m 1 minute</td>
</tr>
<tr>
<td></td>
<td>- 1s 1 second</td>
</tr>
<tr>
<td></td>
<td>- 3.3ms 3.3 ms</td>
</tr>
<tr>
<td></td>
<td>- The default is 10seconds.</td>
</tr>
<tr>
<td>Step 7 end</td>
<td>Exits the interface.</td>
</tr>
</tbody>
</table>
## DETAILED STEPS TO CONFIGURE CFM MEP AND MIP ON A EVC

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable  | Enables privileged EXEC mode.  

**Example:**  
Router> enable  
- Enter your password if prompted.  

| 2    | configure terminal | Enters global configuration mode.  

**Example:**  
Router# configure terminal  

| 3    | interface | Enters the interface mode.  

**Example:**  
Router(config)# interface tengigabitethernet 1/0/0  

| 4    | service instance (id) ethernet (evc-name) | Configures the service instance and the ethernet virtual connections.  

**Example:**  
Router(config-interface)#service instance 41 ethernet 41  

| 5    | encapsulation (encapsulation-type) | Configures the encapsulation type.  

**Example:**  
Router(config-if-srv)#encapsulation dot1q 41  

| 6    | bridge-domain (number) | Configures the bridge domain values. The default domain number is zero; this is the domain number required when communicating to IEEE bridges that do not support this domain extension.  

**Example:**  
Router(config-if)#bridge-domain 41  

| 7    | cfm mep domain (domain-name) mpid (id) | Configures the MEP domain and the ID.  

**Example:**  
Router(config-if-srv)#cfm mep domain L4 mpid 4001  

| 8    | cfm mip level (level) | Automatically creates a MIP in the Ethernet interface and sets the maintenance level number. The acceptable range of maintenance levels is zero to seven.  

**Example:**  
PE1(config-if-srv)#cfm mip level 4
### IEEE 802.1ag-2007 Compliant CFM

#### SUMMARY STEPS TO CONFIGURE CFM MEP AND MIP ON A SWITCH PORT

1. `enable`
2. `configure terminal`
3. `interface`
4. `switchport`
5. `switchport mode {trunk}`
6. `ethernet cfm mep domain domain-name mpid mpid {vlan vlan-id | port}`
   
    or
6. `ethernet cfm mip level {0 to 7} {vlan vlan-id}`
7. `end`

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong> <code>cfm encapsulation</code></td>
<td>Configures the CFM encapsulation type.</td>
</tr>
<tr>
<td><strong>Example:</strong> PE1#(config-if-srv)#cfm encapsulation dot1q 100 second-dot1q 200</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 10** `end` | Exits the service instance interface mode. |
### DETAILED STEPS TO CONFIGURE CFM MEP AND MIP ON A SWITCHPORT

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>interface</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface tengigabitethernet 1/0/0</td>
</tr>
<tr>
<td></td>
<td>Enters the interface mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>switchport</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-interface)#switchport</td>
</tr>
<tr>
<td></td>
<td>Configures the Layer 3 mode into Layer 2 mode for Layer 2 configuration.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>switchport mode (trunk)</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)#switchport mode trunk</td>
</tr>
<tr>
<td></td>
<td>Configures a trunking VLAN Layer 2 interface.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>**ethernet cfm mep domain domain-name mpid mpid {vlan vlan-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)#ethernet cfm mep domain L4 mpid 1 vlan 41</td>
</tr>
<tr>
<td></td>
<td>Sets a port as internal to a maintenance domain, and defines it as a maintenance endpoint. It sets the device into config-if-ecfm-mep configuration mode, where parameters specific to the MEP can be set.</td>
</tr>
<tr>
<td></td>
<td>• domain-name: String, maximum length of 43 characters</td>
</tr>
<tr>
<td></td>
<td>• mpid: 1 to 8191</td>
</tr>
<tr>
<td></td>
<td>• vlan-id: 1 to 4094</td>
</tr>
<tr>
<td></td>
<td>• port: a port MEP, untagged and valid only for outward direction to configure MEP with no VLAN association.</td>
</tr>
</tbody>
</table>

or
IEEE 802.1ag-2007 Compliant CFM

SUMMARY STEPS TO CONFIGURE CFM MEP ON A ROUTED PORT

1. enable
2. configure terminal
3. interface
4. no ip address
5. no mls qos trust
6. ethernet cfm mep domain domain-name mpid mpid {vlan vlan-id}
7. interface gigabitethernet
8. encapsulation dot1Q vlan-id
9. end

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>ethernet cfm mip level (0 to 7) (vlan vlan-id )</td>
</tr>
<tr>
<td>Example:</td>
<td>PE1(config-if)#ethernet cfm mip level 4 vlan 10</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
</tr>
</tbody>
</table>
## Detailed Steps to Configure CFM MEP on a Routed Port

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable  | Enables privileged EXEC mode.  
       |         | • Enter your password if prompted. |
|      | Example:  
       |         | Router> enable |
| 2    | configure terminal | Enters global configuration mode. |
|      | Example:  
       |         | Router# configure terminal |
| 3    | interface | Enters the interface mode. |
|      | Example:  
       |         | Router(config)# interface tengigabitethernet 1/0/0 |
| 4    | no ip address | Removes the configured IP address or disables IP processing. |
|      | Example:  
       |         | Router(config-interface)# no ip address |
| 5    | no mls qos trust | Configures the multilayer switching (MLS) quality of service (QoS) port trust state and traffic by examining the class of service (CoS) or differentiated services code point (DSCP) value. Use the no form of this command to return a port to its untrusted state. |
|      | Example:  
       |         | Router(config-if)# no mls qos trust |
| 6    | ethernet cfm mep domain domain-name mpid mpid (vlan vlan-id) | Sets a port as internal to a maintenance domain, and defines it as a maintenance end point. It sets the device into config-if-ecfm-mep configuration mode, where parameters specific to the MEP can be set.  
       |         | • domain-name: String, maximum length of 43 characters  
       |         | • mpid: 1 to 8191  
       |         | • vlan-id: 1 to 4094  
|      | Example:  
       |         | Router(config-if)#ethernet cfm mep domain routed mpid 4001 vlan 4001 |
| 7    | interface gigabitethernet | Configures the subinterface. |
|      | Example:  
       |         | Router(config)# interface tengigabitethernet 1/0/0.1 |
IEEE 802.1ag-2007 Compliant CFM

Verification

Use the following commands to verify operation.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ethernet cfm maintenance-points local</td>
<td>Displays the local maintenance points.</td>
</tr>
<tr>
<td>Router# show ethernet cfm maintenance-points remote</td>
<td>Displays the remote maintenance end points.</td>
</tr>
<tr>
<td>Router# show ethernet cfm errors</td>
<td>Displays all the CFM Continuity Check error conditions logged on the device.</td>
</tr>
<tr>
<td>Router# show ethernet cfm mpdb</td>
<td>Displays the remote maintenance points.</td>
</tr>
</tbody>
</table>

Example

The following example shows a configuration of MEP in a switchport:

```
ethernet cfm domain L4 level 4
service s41 evc 41 vlan 41
continuity-check
int TenGigabitEthernet2/0/0
switchport
switchport mode trunk
ethernet cfm mep domain L4 mpid 1 vlan 41
```

The following example shows a configuration of MIP in a switchport:

```
ethernet cfm domain L4 level 4
service s41 evc 41 vlan 41
continuity-check
int TenGigabitEthernet2/0/0
switchport
switchport mode trunk
ethernet cfm mip level 4 vlan 10
```

The following example shows a configuration of MEP in an EVC bridge domain:

```
ethernet cfm domain L4 level 4
service s41 evc 41 vlan 41
continuity-check
int TenGigabitEthernet2/0/0
switchport
switchport mode trunk
encapsulation dot1q 41
cfm mep domain L4 mpid 4001
```

The following example shows a configuration of MIP in an EVC bridge domain:

```
ethernet cfm domain L4 level 4
service s41 evc 41 vlan 41
continuity-check
int TenGigabitEthernet2/0/0
```
service instance 41 ethernet 41
encapsulation dot1q 41
bridge-domain 41
cfm cfm mip level 4

The following example shows a configuration of MEP on a routed port:

ethernet cfm domain routed level 5
  service s2 evc 2 vlan 2 direction down
  continuity-check
interface GigabitEthernet8/0/0
  no ip address
  no mls qos trust
  ethernet cfm mep domain routed mpid 4001 vlan 4001
  interface GigabitEthernet8/0/0.10
    encapsulation dot1Q 10

The following example shows CFM configuration over a EVC with cross connect in the global domain configuration mode:

ethernet cfm domain L6 level 6
service xconn evc xconn
continuity-check

The following example shows CFM configuration over a EVC with cross connect in the interface configuration mode:

ethernet cfm domain L6 level 6
  service s100 evc 100
    continuity-check

interface Port-channel10
  no ip address
  service instance 100 ethernet 100
  encapsulation dot1q 200
  xconnect 3.3.3.3 1 encapsulation mpls
  cfm mep domain L6 mpid 602
  cfm mip level 7

CFM over EFP Interface with xconnect

Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance Ethernet layer OAM protocol that includes proactive connectivity monitoring, fault verification, and fault isolation. Currently, Ethernet CFM supports Up facing and Down facing Maintenance Endpoints (MEPs). For information on Ethernet Connectivity Fault Management, see http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srethcfm.html

The CFM over EFP Interface with xconnect feature allows you to:

- Forward continuity check messages (CCM) towards the core over cross connect pseudowires.
- Receive CFM messages from the core.
- Forward CFM messages to the access side (after Continuity Check Database [CCDB] based on maintenance point [MP] filtering rules).

Restrictions and Usage Guidelines

When configuring CFM over EFP Interface with cross connect, follow these restrictions and usage guidelines:

- The following line cards are supported:
  - ES20 line cards
IEEE 802.1ag-2007 Compliant CFM

Chapter 4 Configuring Layer 1 and Layer 2 Features

− ES+ line cards
  • Only a single down-facing MEP is allowed on the L2VFI.
  • As the number of PEs in a VPLS instance scale up, the number of CFM CC messages processed increases. Accordingly, the configuration of the down-facing MEP on L2VFI for large fully meshed PW topologies should be considered for only premium valued networks.
  • In the design of CFM domains, the maintenance level of an Down-facing MEP on the L2VFI interface must be lower than the level from the AC.
  • Up MEP, Down MEP, and MIPs are supported.

Configuring CFM over EFP with xconnect for the Cisco 7600 Router

This section describes how to configure REP over EVC for the Cisco 7600 router:

- Configuring CFM over EFP Interface with Cross Connect—Basic Configuration, page 4-256
- Configuring CFM over EFP Interface with Cross Connect—Single Tag VLAN Cross Connect, page 4-259
- Configuring CFM over EFP Interface with Cross Connect—Double Tag VLAN Cross Connect, page 4-261
- Configuring CFM over EFP Interface with Cross Connect—Selective QinQ Cross Connect, page 4-263
- Configuring CFM over EFP Interface with Cross Connect—Port-Based Cross Connect Tunnel, page 4-264
- Configuring CFM over EFP Interface with Cross Connect—Port Channel-Based Cross Connect Tunnel, page 4-266

Configuring CFM over EFP Interface with Cross Connect—Basic Configuration

This section describes how to configure CFM over EFP Interface with cross connect.

SUMMARY STEPS

1. enable
2. configure terminal
3. pseudowire-class [pw-class-name]
4. encapsulation mpls
5. exit
6. interface gigabitethernet slot/port or interface tengigabitethernet slot/port
7. service instance id {Ethernet [service-name]
8. encapsulation dot1q vlan_id
9. xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual] | mpls [manual]} | pw-class pw-class-name } pw-class pw-class-name [sequencing {transmit | receive | both}]
10. cfm mep domain domain-name [up | down] mpid mpid-value [cos cos-value]
11. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td>pseudowire-class [pw-class-name]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# pseudowire-class vlan-xconnect</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies that Multiprotocol Label Switching (MPLS) is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.</td>
</tr>
<tr>
<td>encapsulation mpls</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# encapsulation mpls</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Exits the pseudowire class configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-srv)# exit</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure.</td>
</tr>
<tr>
<td>interface gigabitethernet slot/port or</td>
<td></td>
</tr>
<tr>
<td>interface tengigabitethernet slot/port</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-srv)# interface Gi2/0/2</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td>service instance id ethernet [service-name]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-srv)# service instance 101 ethernet</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Configures the encapsulation. Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface for the appropriate service instance.</td>
</tr>
<tr>
<td>encapsulation dot1q (any</td>
<td>vlan-id[vlan-id[-vlan-id]]) second-dot1q (any</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if-srv)# encapsulation dot1q 100 second dot1q 200</td>
</tr>
</tbody>
</table>
IEEE 802.1ag-2007 Compliant CFM

Chapter 4 Configuring Layer 1 and Layer 2 Features

IEEE 802.1ag-2007 Compliant CFM

Examples

**Step 9**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>xconnect peer-ip-address vc-id {encapsulation (l2tpv3 [manual]</td>
<td>mpls [manual])</td>
</tr>
</tbody>
</table>

Example:

Router(config-if-srv)# xconnect 10.0.3.201 123 pw-class vlan-xconnect

**Step 10**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>cfm mep domain domain-name [up</td>
<td>down] mpid mpid-value [cos cos-value]</td>
</tr>
</tbody>
</table>

Example:

Router(config-if-srv)# cfm mep down mpid 100 domain Core

**Step 11**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits the interface configuration mode.</td>
</tr>
</tbody>
</table>

Example:

Router(config-if-srv)# exit

**Examples**

This example shows how to configure CFM over EVC using cross connect.

PE1# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE1(config)# ethernet cfm domain L6 level 6
PE1(config-ecfm)# service s256 evc 256
PE1(config-ecfm-srv)# continuity-check
PE1(config-ecfm-srv)# end

PE1(config)# int ten 2/0/0
PE1(config-if)# no ip address
PE1(config-if)# service instance 256 ethernet 256
PE1(config-if-srv)# encapsulation dot1q 256
PE1(config-if-srv)# xconnect 1.1.1.1 1 encapsulation mpls
PE1(config-if-ether-vc-xconn)# cfm mep domain L6 mpid 256
PE1(config-if-srv-ecfm-mep)# end

PE1#
PE1(config)# ethernet cfm domain L2 level 2
PE1(config-ecfm)# service s256 evc 256 direction down
PE1(config-ecfm-srv)# continuity-check
PE1(config-ecfm-srv)# end
PE1#
PE1(config)# int ten 2/0/0
PE1(config-if)# no ip address
PE1(config-if)# service instance 256 ethernet 256
PE1(config-if-srv)# encapsulation dot1q 256
PE1(config-if-srv)# xconnect 1.1.1.1 1 encapsulation mpls
PE1(config-if-ether-vc-xconn)# cfm mep domain L6 mpid 256
PE1(config-if-srv-ecfm-mep)# end
PE1#
Configuring CFM over EFP Interface with Cross Connect—Single Tag VLAN Cross Connect

This section describes how to configure CFM over EFP Interface with Single Tag VLAN cross connect.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot/subslot/port or interface tengigabitethernet slot/port`
4. `service instance id {Ethernet [service-name]}`
5. `encapsulation dot1q {any | vlan-id[vlan-id]} second-dot1q {any | vlan-id[vlan-id]}`
6. `rewrite ingress tag [push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id | dot1ad vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} [symmetric]}
7. `xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual] | mpls [manual]} | pw-class pw-class-name }[pw-class pw-class-name] [sequencing {transmit | receive | both}]`
8. `cfm mep domain domain-name [up | down] mpid mpid-value [cos cos-value]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface gigabitethernet slot/subslot/port</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface Gi2/0/2</td>
</tr>
<tr>
<td></td>
<td>Specifies the Gigabit Ethernet interface to configure, where: slot/subslot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>service instance id Ethernet [service-name]</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# service instance 101 ethernet</td>
</tr>
<tr>
<td></td>
<td>Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
</tbody>
</table>
IEEE 802.1ag-2007 Compliant CFM

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>`encapsulation dot1q {any</td>
<td>vlan-id[vlan-id[-vlan-id]]} second-dot1q {any</td>
</tr>
<tr>
<td>6</td>
<td>`rewrite ingress tag {push {dot1q vlan-id</td>
<td>dot1q vlan-id second-dot1q vlan-id</td>
</tr>
<tr>
<td>7</td>
<td>`xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual]</td>
<td>mpls [manual]}</td>
</tr>
<tr>
<td>8</td>
<td>`cfm mep domain domain-name [up</td>
<td>down] mpid mpid-value [cos cos-value]`</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure CFM over EFP Interface with Single Tag VLAN cross connect:

```
PE3(config)#ethernet cfm domain L2 level 2
PE3(config-ecfm)# service s256 evc 256 direction down
PE3(config-ecfm-srv)# continuity-check
PE3(config-ecfm-srv)#end
PE3#
PE3(config)#int ten 2/0/0
PE3(config-if)#no ip address
PE3(config-if)# service instance 256 ethernet 256
PE3(config-if-srv)# encapsulation dot1q 256
PE3(config-if-srv)# xconnect 1.1.1.1 1 encapsulation mpls
PE3(config-if-ether-vc-xconn)# cfm mep domain L6 mpid 256
PE3(config-if-srv-ecfm-mep)#end
PE3#
```
Configuring CFM over EFP Interface with Cross Connect—Double Tag VLAN Cross Connect

This section describes how to configure CFM over EFP Interface with Double Tag VLAN cross connect.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/subslot/port
4. service instance id {Ethernet [service-name]}
5. encapsulation dot1q {any | vlan-id[vlan-id][vlan-id]} second-dot1q {any
   vlan-id[vlan-id][vlan-id]}
6. rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id}
   | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} 2-to-1 dot1q
   vlan-id | dot1ad vlan-id} 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q
   vlan-id} 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} } [symmetric]
7. xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual] | mpls [manual]} | pw-class
   pw-class-name }[pw-class pw-class-name] [sequencing {transmit | receive | both}]
8. cfm mep domain domain-name [up | down] mpid mpid-value [cos cos-value]
9. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>· Enter your password if prompted.</td>
</tr>
<tr>
<td>Router# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
| Step 3 interface gigabitethernet slot/subslot/port | Specifies the Gigabit Ethernet interface to configure, where:
| Example:                  | · slot/subslot/port—Specifies the location of the interface.           |
| Router(config)# interface Gi2/0/2 |                                                                          |
| Step 4 service instance id Ethernet [service-name] | Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode. |
| Example:                  |                                                                          |
| Router(config-if)# service instance 100 ethernet |                                                                          |
### IEEE 802.1ag-2007 Compliant CFM

#### Command Purpose

**Step 5**
- **encapsulation dot1q (any | vlan-id[vlan-id[-vlan-id]]) second-dot1q (any | vlan-id[vlan-id[-vlan-id]])**

  **Example:**
  ```
  Router(config-if-srv)# encapsulation dot1q 100 second-dot1q 200
  ```

  Configures the encapsulation. Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface for the appropriate service instance.

**Step 6**
- **rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 (dot1q vlan-id | dot1ad vlan-id)| 2-to-1 (dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id) | 1-to-2 (dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id) | 2-to-2 (dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id)} [symmetric]}

  **Example:**
  ```
  Router(config-if-srv)# rewrite dot1q double symmetric
  ```

  Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.

**Step 7**
- **xconnect peer-ip-address vc-id (encapsulation {l2tpv3 [manual] | mpls [manual]} | pw-class pw-class-name) [pw-class pw-class-name] [sequencing {transmit | receive | both}]

  **Example:**
  ```
  Router(config)# xconnect 1.1.1.1 100 pw-class vlan-xconnect
  ```

  Binds an attachment circuit to a pseudowire, and configures an Any Transport over MPLS (AToM) static pseudowire.

**Step 8**
- **cfm mep domain domain-name [up | down] mpid mpid-value [cos cos-value]

  **Example:**
  ```
  Router# cfm mep down mpid 100 domain Core
  ```

  Configures a maintenance endpoint (MEP) for a domain.

### Examples

This example shows how to configure CFM over EFP Interface with Double Tag VLAN cross connect:

```bash
PE1(config)# ethernet cfm domain L2 level 2
PE1(config-ecfm)# service s256 evc 256 direction down
PE1(config-ecfm-srv)# continuity-check
PE1(config-ecfm-srv)#end
PE1#
PE1(config)#int ten 2/0/0
PE1(config-if)#no ip address
PE1(config-if)# service instance 256 ethernet 256
PE1(config-if-srv)# encapsulation dot1q 256 second-dot1q 257
PE1(config-if-srv)# xconnect 1.1.1.1 1 encapsulation mpls
PE1(config-if-ether-vc-xconn)# cfm mep domain L6 mpid 256
PE1(config-if-srv-ecfm-mep)#end
```
Configuring CFM over EFP Interface with Cross Connect—Selective QinQ Cross Connect

This section describes how to configure CFM over EFP Interface with Selective QinQ cross connect.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/subslot/port
4. exit
5. service instance id {Ethernet [service-name]}
6. encapsulation dot1q {any | vlan-id[vlan-id][vlan-id]} second-dot1q {any vlan-id[vlan-id][vlan-id]}
7. xconnect peer-ip-address vc-id {encapsulation [l2tpv3 [manual] | mpls [manual]] | pw-class pw-class-name } [pw-class pw-class-name] [sequencing {transmit | receive | both}]
8. cfm mep domain domain-name [up | down] mpid mpid-value [cos cos-value]
9. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted.  
  Example:  
  Router# enable |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  Router# configure terminal |
| **Step 3** interface gigabitethernet slot/sub-slot/port | Specifies the Gigabit Ethernet interface to configure, where:  
  slot/subslot/port—Specifies the location of the interface.  
  Example:  
  Router(config)# interface Gi2/0/2 |
| **Step 4** service instance id Ethernet [service-name] | Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.  
  Example:  
  Router(config-if)# service instance 101 ethernet |
IEEE 802.1ag-2007 Compliant CFM

Chapter 4  Configuring Layer 1 and Layer 2 Features

IEEE 802.1ag-2007 Compliant CFM

Examples

This example shows how to configure CFM over EFP Interface with Selective QinQ cross connect:

PE1(config)#ethernet cfm domain L2 level 2
PE1(config-ecfm)# service s256 evc 256 direction down
PE1(config-ecfm-srv)#  continuity-check
PE1(config-ecfm-srv)#end

Step 5

**Command**

```
encapsulation dot1q {any | vlan-id[vlan-id[-vlan-id]]} second-dot1q {any | vlan-id[vlan-id[-vlan-id]]}
```

**Purpose**

Configures the encapsulation. Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface for the appropriate service instance.

**Example:**

```
Router(config-if-srv)# encapsulation default
```

Step 6

**Command**

```
xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual] | mpls [manual] } [pw-class pw-class-name]} [sequencing {transmit | receive | both}]
```

**Purpose**

Binds an attachment circuit to a pseudowire, and configures an Any Transport over MPLS (AToM) static pseudowire.

**Example:**

```
Router(config)# xconnect 10.0.3.201 123 pw-class vlan-xconnect
```

Step 7

**Command**

```
cfm mep domain domain-name [up | down] mpid mpid-value [cos cos-value]
```

**Purpose**

Configures a maintenance endpoint (MEP) for a domain.

**Example:**

```
Router# cfm mep down mpid 100 domain Core
```

Examples

This example shows how to configure CFM over EFP Interface with Selective QinQ cross connect:

```
PE1(config)#ethernet cfm domain L2 level 2
PE1(config-ecfm)# service s256 evc 256 direction down
PE1(config-ecfm-srv)#  continuity-check
PE1(config-ecfm-srv)#end
PE1#  
PE1(config)#int ten 2/0/0
PE1(config-if)#no ip address
PE1(config-if)# service instance 256 ethernet 256
PE1(config-if-srv)#  encapsulation dot1q 256 second-dot1q 257 cos 7
PE1(config-if-srv)# xconnect 1.1.1.1 1 encapsulation mpls
PE1(cfg-if-ether-vc-xconn)#  cfm mep domain L6 mpid 256
PE1(config-if-srv-ecfm-mep)#end
PE1#
```

Configuring CFM over EFP Interface with Cross Connect—Port-Based Cross Connect Tunnel

This section describes how to configure CFM over EFP Interface with Port-Based cross connect Tunnel.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/subslot/port
4. service instance id {Ethernet [service-name]}

```
```

```
5. `encapsulation dot1q {any | vlan-id[vlan-id[vlan-id]]} second-dot1q {any | vlan-id[vlan-id[vlan-id]]}

6. `xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual] | mpls [manual]} | pw-class [pw-class-name] [pw-class pw-class-name] [sequencing {transmit | receive | both}]`

7. `cfm mep domain domain-name [up | down] mpid mpid-value [cos cos-value]

8. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface gigabitethernet slot/sub-slot/port</td>
<td>Specifies the Gigabit Ethernet interface to configure, where: slot/subslot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# interface Gi2/0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id Ethernet [service-name]</td>
<td>Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# service instance 100 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation dot1q (any</td>
<td>vlan-id[vlan-id[-vlan-id]]) second-dot1q (any</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if-srv)# encapsulation dot1q 10-20, 30, 50-60</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4 Configuring Layer 1 and Layer 2 Features

IEEE 802.1ag-2007 Compliant CFM

Examples

This example shows how to configure CFM over EFP Interface with Port-Based cross connect Tunnel:

```
PE3(config)# ethernet cfm domain L2 level 2
PE3(config-ecfm)# service s256 evc 256 direction down
PE3(config-ecfm-srv)# continuity-check
PE3(config-ecfm-srv)#
PE3(config)#
PE3(config)# int ten 2/0/0
PE3(config-if)# no ip address
PE3(config-if)# service instance 256 ethernet 256
PE3(config-if-srv)# encapsulation dot1q 256
PE3(config-if-srv)#
PE3(config-if-srv-ecfm-mep)#
PE3(config-if-srv-ecfm-mep)#
PE3(config-if-srv-ecfm-mep-vc)#
```

Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>xconnect peer-ip-address vc-id [encapsulation (l2tpv3 [manual]</td>
<td>mpls [manual])</td>
</tr>
</tbody>
</table>

Example:

```
Router(config)# xconnect 1.1.1.1 100
pw-class vlan-xconnect
```

Step 7

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>cfm mep domain domain-name [up</td>
<td>down] mpid mpid-value [cos cos-value]</td>
</tr>
</tbody>
</table>

Example:

```
Router# cfm mep up mpid 100 domain Core
```

Configuring CFM over EFP Interface with Cross Connect—Port Channel-Based Cross Connect Tunnel

This section describes how to configure CFM over EFP Interface with Port Channel-Based cross connect Tunnel.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/subslot/port
4. service instance id [Ethernet] [service-name]
5. encapsulation dot1q [anyvlan-id[vlans-id[vlan-id]]] second-dot1q [anyvlan-id[vlans-id[vlan-id]]]
6. `rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id | dot1ad vlan-id second-dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id}} [symmetric]

7. `xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual] | mpls [manual]} | pw-class pw-class-name} [pw-class pw-class-name] [sequencing {transmit | receive | both}]

8. `cfm mep domain domain-name [up | down] mpid mpid-value [cos cos-value]

9. `exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# enable</td>
</tr>
<tr>
<td>Enables privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface gigabitethernet slot/sub-slot/port</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface Port-channel 1</td>
</tr>
<tr>
<td>Specifies the Gigabit Ethernet interface to configure, where: slot/subslot/port—Specifies the location of the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>service instance id Ethernet [service-name]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# service instance 101 ethernet</td>
</tr>
<tr>
<td>Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>encapsulation dot1q {any</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if-srv)# encapsulation dot1q 20 second-dot1q 30</td>
</tr>
<tr>
<td>Configures the encapsulation. Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface for the appropriate service instance.</td>
<td></td>
</tr>
</tbody>
</table>
### IEEE 802.1ag-2007 Compliant CFM

#### Examples

This example shows how to configure CFM over EFP Interface with Port Channel-Based cross connect Tunnel:

```
PE3(config)#ethernet cfm domain L2 level 2
PE3(config-ecfm)# service s256 evc 256 direction down
PE3(config-ecfm-srv)# continuity-check
PE3(config-ecfm-srv)#end
PE3#
PE3(config)#int port-20
PE3(config-if)#no ip address
PE3(config-if)# service instance 256 ethernet 256
PE3(config-if-srv)# encapsulation dot1q 256
PE3(config-if-srv)# xconnect 1.1.1.1 1 encapsulation mpls
PE3(config-if-srv-ecfm-mep)# cfm mep domain L6 mpid 256
PE3(config-if-srv-ecfm-mep)#end
```

#### Verification

Use the following commands to verify a configuration:

- Use the `show ethernet cfm ma remote` commands to verify the CFM over EVC configuration. This command shows the basic configuration information for CFM.

```
Router-30-PE1#show ethernet cfm ma local
```
## Local MEPs:

<table>
<thead>
<tr>
<th>MPID</th>
<th>Domain Name</th>
<th>Lvl</th>
<th>MacAddress</th>
<th>Type</th>
<th>CC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>L6</td>
<td>6</td>
<td>000a.f393.56d0</td>
<td>XCON</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>L5</td>
<td>5</td>
<td>0007.8478.4410</td>
<td>XCON</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Local MEPs: 2

## Local MIPs:

<table>
<thead>
<tr>
<th>Level</th>
<th>Port</th>
<th>MacAddress</th>
<th>SrvcInst</th>
<th>Type</th>
<th>Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Te2/0/0</td>
<td>0007.8478.4410</td>
<td>1</td>
<td>XCON</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Total Local MIPs: 1

- Use the `show ethernet cfm ma remote` to verify the MEP configuration:

```plaintext
Router-30-PE1#show ethernet cfm ma remote
```

<table>
<thead>
<tr>
<th>MPID</th>
<th>Domain Name</th>
<th>Lvl</th>
<th>Port</th>
<th>MacAddress</th>
<th>Ingress</th>
<th>IfSt</th>
<th>PtSt</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>L5</td>
<td>5</td>
<td>Te2/0/0</td>
<td>000a.f393.56d0</td>
<td>Up</td>
<td>Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>L5</td>
<td>5</td>
<td>Te2/0/0:(2.2.2.2, 1)</td>
<td>XCON</td>
<td>N/A</td>
<td>1</td>
<td>9s</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>L6</td>
<td>6</td>
<td>Te2/0/0:(2.2.2.2, 1)</td>
<td>XCON</td>
<td>N/A</td>
<td>1</td>
<td>1s</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Remote MEPs: 2

- Use the `show ethernet cfm mpdb` command to verify the catologue of CC with MIP in intermediate routers.

```plaintext
PE2#show ethernet cfm mpdb
```

<table>
<thead>
<tr>
<th>MPID</th>
<th>Domain Name</th>
<th>Lvl</th>
<th>Domain ID</th>
<th>Ingress</th>
<th>Type</th>
<th>SrvcInst</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>600</td>
<td>L6</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IEEE-CFM</td>
</tr>
<tr>
<td>700</td>
<td>L7</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IEEE-CFM</td>
</tr>
</tbody>
</table>
IEEE 802.1ag-2007 Compliant CFM

Chapter 4  Configuring Layer 1 and Layer 2 Features

- Use the `show mpls l2 transport vc 1 detail` command to show detailed configuration information:

  ```
  PE1#sh mpls l2 vc 1 detail
  Local interface: Te8/0/1 up, line protocol up, Eth VLAN 200 up
  Interworking type is Ethernet
  Destination address: 3.3.3.3, VC ID: 1, VC status: up
  Output interface: Te8/0/0, imposed label stack {21}
  Preferred path: not configured
  Default path: active
  Next hop: 20.1.1.2
  Create time: 21:13:27, last status change time: 02:55:33
  Signaling protocol: LDP, peer 3.3.3.3:0 up
  Targeted Hello: 2.2.2.2(LDP Id) -> 3.3.3.3, LDP is UP
  Status TLV support (local/remote) : enabled/supported
  LDP route watch : enabled
  Last local dataplane status rcvd: No fault
  Last local SSS circuit status rcvd: No fault
  Last local SSS circuit status sent: No fault
  Last local LDP TLV status sent: No fault
  Last remote LDP TLV status rcvd: No fault
  Last remote LDP ADJ status rcvd: No fault
  MPLS VC labels: local 21, remote 21
  Group ID: local 0, remote 0
  MTU: local 1500, remote 1500
  Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  VC statistics:
  transit packet totals: receive 37, send 1067452272
  transit byte totals: receive 4181, send 72586757556
  transit packet drops: receive 0, seq error 0, send 0
```

- Use `show mpls forwarding-table` command to verify the cross connect VC:

  ```
  PE1#show mpls forwarding-table
  Local      Outgoing Prefix          Bytes Label  Outgoing   Next Hop
  Label      Label or Tunnel Id       Switched      interface
  17         Pop Label  3.3.3.3/32     23038746624 Te8/0/0    20.1.1.2
  21         No Label   l2ckt(1)       4181          Te8/0/1    point2point
  ```

- Use `show ethernet cfm error` command to view the error report:

  ```
  PE2#show ethernet cfm error
  --------------------------------------------------------------------------------
  MPID Domain Id    MAC Address     Type   Id   Lvl     Reason   Age
  MAName
  --------------------------------------------------------------------------------
  - L3  001d.45fe.ca81  BD-V    200   3  Receive AIS   8s
  s2
  PE2#
  ```
**Configuring CFM over EFP Interface with xconnect—Port Channel-Based xconnect Tunnel**

Use the following commands at the customer facing port:

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface type slot/subslot/port**
4. **service instance id {Ethernet [service-name]}**
5. **encapsulation untagged | dot1q {any | vlan-id[vlan-id][vlan-id]} second-dot1q {any | vlan-id[vlan-id][vlan-id]}**
6. **rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 | dot1q vlan-id | dot1ad vlan-id | 2-to-1 dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id}}**
7. **xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual] | mpls [manual]} | pw-class pw-class-name }[pw-class pw-class-name] [sequencing {transmit | receive | both}]**
8. **cfm mep domain domain-name mpid mpid-value [cos cos-value]**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>interface gigabitethernet slot/subslot/port</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config)# interface Port-channel 1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>service instance id Ethernet [service-name]</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config-if)# service instance 101 ethernet</td>
</tr>
</tbody>
</table>
### Examples

This example shows how to configure CFM over EFP Interface with Port Channel-Based xconnect Tunnel:

```
PE3(config)# ethernet cfm domain L2 level 2
PE3(config-ecfm)# service s256 evc 256 direction down
PE3(config-ecfm-srv)# continuity-check
PE3(config-ecfm-srv)# end
PE3#
PE3(config)# int port-20
PE3(config-if)# no ip address
PE3(config-if)# service instance 256 ethernet 256
PE3(config-if-srv)# encapsulation dot1q 256
PE3(config-if-srv)# xconnect 1.1.1.1 1 encapsulation mpls
PE3(config-if-srv-ether-vc-xconn)# cfm mep domain L6 mpid 256
PE3(config-if-srv-ecfm-mep)# end
```

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><strong>encapsulation untagged dot1q</strong> *(any</td>
<td>vlan-id[vlan-id[vlan-id]])* <strong>second-dot1q</strong> *(any</td>
</tr>
<tr>
<td>6</td>
<td><strong>rewrite ingress tag</strong> *(push {dot1q vlan-id</td>
<td>dot1q vlan-id second-dot1q vlan-id</td>
</tr>
<tr>
<td>7</td>
<td><strong>xconnect peer-ip-address vc-id</strong> *(encapsulation {l2tpv3 [manual]</td>
<td>mpls [manual]}</td>
</tr>
<tr>
<td>8</td>
<td><strong>cfm mep domain</strong> domain-name [up</td>
<td>down] <strong>mpid</strong> mpid-value [cos cos-value]</td>
</tr>
</tbody>
</table>
Verification

Use the following commands to verify a configuration:

- Use `show ethernet cfm ma remote` commands to verify the CFM over EFP configuration. This command shows the basic configuration information for CFM.

  
  ```
  Router-30-PE1#show ethernet cfm ma local
  Local MEPs:
  +---------------------------------------------------------------------------+-
  | MPID | Domain Name | Domain Id | MA Name | EVC name | Lvl | MacAddress | Type | CC |
  +---------------------------------------------------------------------------+-
  | 1    | L6          | 6         | 000a.f393.56d0 | XCON | Y |
  | 3    | L5          | 5         | 0007.8478.4410 | XCON | Y |
  +---------------------------------------------------------------------------+-
  Total Local MEPs: 2
  
  Local MIPs:
  * = MIP Manually Configured
  +---------------------------------------------------------------------------+-
  | Level | Port | MacAddress | SrvcInst | Type | Id |
  +---------------------------------------------------------------------------+-
  | 7     | Te2/0/0 | 0007.8478.4410 | 1 | XCON | N/A |
  +---------------------------------------------------------------------------+-
  Total Local MIPs: 1
  ```

- Use `show ethernet cfm ma remote` to verify the MEP configuration:

  ```
  Router-30-PE1#show ethernet cfm ma remote
  +---------------------------------------------------------------------------+-
  | MPID | Domain Name | Domain Id | MA Name | EVC name | Lvl | MacAddress | Type | Id | SrvcInst | Age |
  +---------------------------------------------------------------------------+-
  | 4    | L5          | 000a.f393.56d0 | Up | Up |
  | 5    | L5          | Te2/0/0:(2.2.2.2, 1) | XCON | N/A | 1 |
  | 2    | L6          | 000a.f393.56d0 | Up | Up |
  | 6    | L6          | Te2/0/0:(2.2.2.2, 1) | XCON | N/A | 1 |
  +---------------------------------------------------------------------------+-
  Total Remote MEPs: 2
  ```

- Use `show ethernet cfm mpdb` command to verify the catalogue of CC with MIP in intermediate routers.

  ```
  PE2#show ethernet cfm mpdb
  * = Can Ping/Traceroute to MEP
  +---------------------------------------------------------------------------+-
  | MPID | Domain Name | Domain ID | Ingress | Type | Id | SrvcInst | Age |
  +---------------------------------------------------------------------------+-
  | 4    | L5          | 000a.f393.56d0 | Up | Up |
  | 5    | L5          | Te2/0/0:(2.2.2.2, 1) | XCON | N/A | 1 |
  +---------------------------------------------------------------------------+-
  Total Remote MEPs: 2
  ```
IEEE 802.1ag-2007 Compliant CFM

Chapter 4  Configuring Layer 1 and Layer 2 Features

IEEE 802.1ag-2007 Compliant CFM

<table>
<thead>
<tr>
<th>Expd</th>
<th>MA Name</th>
<th>EVC Name</th>
<th>Type Id</th>
<th>SrvcInst</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>600</td>
<td>L6</td>
<td>0021.d8ca.d7d0</td>
<td>IEEE-CFM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>L6</td>
<td>Te2/1:(2.2.2.2, 1)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>s1</td>
<td>XCON N/A</td>
<td>2s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>700</td>
<td>L7</td>
<td>001f.cab7.fd01</td>
<td>IEEE-CFM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>L7</td>
<td>Te2/1:(2.2.2.2, 1)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>s1</td>
<td>XCON N/A</td>
<td>3s</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Remote MEPs: 2

- Use `show mpls l2 transport vc 1 detail` command to show detailed configuration information:

PE1#sh mpls l2 transport vc 1 detail
Local interface: Te8/0/1 up, line protocol up, Eth VLAN 200 up
Interworking type is Ethernet
Destination address: 3.3.3.3, VC ID: 1, VC status: up
Output interface: Te8/0/0, imposed label stack {21}
Preferred path: not configured
Default path: active
Next hop: 20.1.1.2
Create time: 21:13:27, last status change time: 02:55:33
Signaling protocol: LDP, peer 3.3.3.3:0 up
Targeted Hello: 2.2.2.2(LDP Id) -> 3.3.3.3, LDP is UP
Status TLV support (local/remote) : enabled/Supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last local SSS circuit status rcvd: No fault
Last local SSS circuit status sent: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 21, remote 21
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description:
Sequencing: receive disabled, send disabled
Control Word: On (configured: autosense)
VC statistics:
transit packet totals: receive 37, send 1067452272
transit byte totals: receive 4181, send 72586757556
transit packet drops: receive 0, seq error 0, send 0

- Use `show mpls forwarding-table` command to verify the xconnect VC:

PE1#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
17         Pop Label  3.3.3.3/32       23038746624   Te8/0/0    20.1.1.2
21         No Label   l2ckt(1)         4181          Te8/0/1    point2point

- Use `show ethernet cfm error` command to view the error report:

PE2#show ethernet cfm error

<table>
<thead>
<tr>
<th>MPID Domain Id</th>
<th>Mac Address</th>
<th>Type Id</th>
<th>Lvl</th>
<th>MAName</th>
<th>Reason</th>
<th>Age</th>
</tr>
</thead>
</table>
Troubleshooting CFM Features

Table 4-33 provides troubleshooting solutions for the CFM features.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| When you configure CFM, the message “Match registers are not available” is displayed. | Use the `show platform mrm info` command on the SP console to verify the match registers. Based on the derived output, perform these tasks:
1. Check if the line card supports the CFM feature.
2. Enable CFM across the system to allow co-existence with other protocols.
3. Ensure that no CFM traffic is present in any supervisor or ports.
4. Configure STP mode to Multiple Spanning Tree (MST) and re-enable CFM or disable CFM completely. For more information on match registers, see **Ethernet Connectivity Fault Management** at [http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srethcfm.html](http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srethcfm.html). CFM uses two match registers to identify the control packet type and each VLAN spanning tree also uses a match register to identify its control packet type. For both protocols to work on the same system, each line card should support three match registers, and at least one supporting only a 44 bit MAC match. |
| CFM configuration errors | CFM configuration error occurs when a MEP receives a continuity check with an overlapping MPID. To verify the source of the error, use the command `show ethernet cfm errors configuration` or `show ethernet cfm errors`. |
| CFM ping and traceroute result is "not found" | Complete these steps:
1. Use `show run ethernet cfm` to view all CFM global configurations.
2. Use `show ethernet cfm location main` to view local MEPs and their CCM statistics
3. Use `show ethernet cfm peer meps` command to View CFM CCM received from Peer MEPs.
4. Use `trace ethernet cfm` command to start a CFM trace. |
## 802.1ah: Configuring the MAC Tunneling Protocol

The MAC Tunneling Protocol (MTP) feature is based on the IEEE 802.1ah standard and provides VLAN and MAC scalability. This feature extends the Cisco QinQ (the IEEE 802.1ad standard) capability to support highly scalable Provider Backbone Architecture (PBA). MTP allows a service provider to interconnect multiple Provider Bridged Networks (PBNs) that support a minimum 10,48,576 (2 to the 20th power) Service VLANS and extend the MAC address scalability.

### Problem

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFM connectivity is down and issues at the maintenance domain levels</td>
<td>Use the `ping ethernet {mac-address</td>
</tr>
<tr>
<td>Loop trap error</td>
<td>Use the <strong>show ethernet cfm error</strong> command to check for Loop Trap errors as shown here:</td>
</tr>
<tr>
<td></td>
<td>CE(config-if)#do sh ethernet cfm err</td>
</tr>
<tr>
<td></td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td>Level Vlan MPID Remote MAC Reason Service ID</td>
</tr>
<tr>
<td></td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td>5 711 550 1001.1001.1001 Loop Trap Error OUT</td>
</tr>
<tr>
<td></td>
<td>PE#sh ethernet cfm err</td>
</tr>
<tr>
<td></td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td>Level Vlan MPID Remote MAC Reason Service ID</td>
</tr>
<tr>
<td></td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td>5 711 550 1001.1001.1001 Loop Trap Error OUT</td>
</tr>
<tr>
<td>Module has insufficient match registers</td>
<td>Complete these steps:</td>
</tr>
<tr>
<td></td>
<td>1. Verify and confirm if a unsupported line card is inserted into the router.</td>
</tr>
<tr>
<td></td>
<td>2. If yes, perform an OIR of the unsupported line card.</td>
</tr>
<tr>
<td>CFM is deactivated</td>
<td>Complete these steps:</td>
</tr>
<tr>
<td></td>
<td>1. Check if all the line cards have free match registers.</td>
</tr>
<tr>
<td></td>
<td>2. Check if CFM is activated on supervisor cards. CFM is not supported on supervisor cards that has two match registers. In this scenario, CFM is automatically disabled on the SUP ports and enabled on the remaining line cards.</td>
</tr>
<tr>
<td>ethernet cfm logging</td>
<td>In a scale scenario, you configure either the console logging rate-limiting using <strong>logging rate-limit</strong> or using <strong>logging buffered</strong> instead of using <strong>logging console</strong>. The suggested rate-limit is around 30 messages per second.</td>
</tr>
</tbody>
</table>
With this feature, you can scale a Provider Bridged P802.1ad network using an existing Bridged and Virtual Bridged Local Area Network (VLAN) deployment. Although the current Cisco QinQ capability provides VLAN scaling, this feature extends the scaling and interoperability between multiple vendors. Bridges in a Provider Backbone Bridged Network (PBBN) need to learn the MAC address of each host to make forwarding decisions. MTP resolves this need for MAC address learning by encapsulating both the data packet and MAC addresses (source and destination) into a new Ethernet frame. The header of the new Ethernet frame contains:

- Destination Backbone MAC (B-MAC)
- Source Backbone MAC (B-MAC)
- Backbone VLAN TAG (B-TAG) with 12-bit Backbone VLAN ID (B-VID)
- Service Instance TAG (I-TAG) with 24-bit Service Instance ID (I-SID)

The MAC scalability is implemented using the B-MACs. Since the new Ethernet frames are encapsulated with MAC address (host) while traversing the PBBN, a bridge needs to learn the B-MACs only. The MAC addresses of hosts are hidden from the Provider Backbone Bridges (PBB), resulting in the PBB Bridges to learn only the provider MAC address, irrespective of the number of hosts or the number of host MAC addresses supported. Since the data packets are sent to specific MAC addresses, the 802.1ah cloud is not flooded with unnecessary traffic. A MAC address is a static entry in the MAC address table on the Backbone Core Bridge.

The VLAN scalability is implemented using the I-SID. The MTP achieves VLAN scalability by using a backbone VLAN TAG with a 12-bit B-VID and the Service Instance TAG with a 24-bit Service Instance ID to provide the VLAN scalability necessary to map large number of customers.

Figure 4-10 shows the basic MTP network deployment.

**Figure 4-10  MTP Network Deployment**

![MTP Network Deployment Diagram]

**MTP Software Architecture**

The encapsulation and decapsulation of MAC addresses is performed on a Backbone Edge Bridge (BEB) at the edge of the PBBN. A BEB can be an I-Bridge (I-BEB), a B-Bridge (B-BEB), or an IB-Bridge (IB-BEB). Currently, MTP is supported only with the IB-BEB functionality.

Figure 4-11 shows the MTP software architecture.

**Figure 4-11  MTP Software Architecture**
IB Backbone Edge Bridge

An IB-BEB consists of one B-Component and one or more I-Components. The IB-BEB provides the functionality to select the B-MAC and insert I-SIDs based on the supported tags. It also validates the I-SIDs and transmits or receives the frames on the B-VLAN.

The iIEEE 802.1ah draft describes two types of customer-facing interfaces supported by IB-BEB:

- **S-Tagged Service Interface**
  - Translating S-tagged Interface
  - Bundling S-tagged interface:
- **Port-Based (transparent) Service Interface**

MTP supports both type of interfaces.

Data Plane Processing

The packets on the ingress EFP are tunneled to the appropriate MAC tunnel using the C-MAC bridge domain. For multiple EFPs using the same I-SID, the switching among EFPs is done using the C-MAC bridge domain. Local switching is performed across all the ports in the bridge domain even if they span multiple tunnel engines.

MTP Configuration

Table 4-34 lists the relationship between the various entities in a Cisco 7600 Series Router for MTP implementation.
Table 4-34  Relationship Between the Various Entities in a Cisco 7600 Series Router

<table>
<thead>
<tr>
<th>Entity to Entity</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFP to C-MAC bridge domain</td>
<td>many to one</td>
</tr>
<tr>
<td>C-MAC bridge domain to I-SID</td>
<td>one to one</td>
</tr>
<tr>
<td>I-SID to B-MAC bridge domain</td>
<td>many to one</td>
</tr>
</tbody>
</table>

Figure 4-12 show N to N relationship within a Cisco 7600 Series Router:

![N to N relationship within a Cisco 7600 Series Router](image)

**Scalability Information**

Table 4-35 lists scalability information for MTP.

Table 4-35  Scalability Information for MTP

<table>
<thead>
<tr>
<th>Scalability Factor</th>
<th>Scalability Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of EVCs in the system</td>
<td>32000</td>
</tr>
<tr>
<td>Number of EVCs per linecard</td>
<td>16000</td>
</tr>
<tr>
<td>Number of C-MAC addresses per NPU</td>
<td>32000 per NPU</td>
</tr>
<tr>
<td>Number of EVCs per C-BD per NPU</td>
<td>110</td>
</tr>
<tr>
<td>Number of B-bridge-domains per chassis</td>
<td>4094</td>
</tr>
<tr>
<td>Number of I-SIDs or MAC-Tunnels</td>
<td>16000</td>
</tr>
<tr>
<td>Number of MAC entries in a C-MAC table</td>
<td>32000</td>
</tr>
</tbody>
</table>
Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines when configuring the MAC Tunneling Protocol on an ES40 line card:

- By default, all the BPDUs are dropped.
- Port channels with 802.1ah EVCs are not supported.
- IGMP Snooping or any multicast protocol support on the C bridge-domain.
- MAC address synchronization and MAC address move notification in the C bridge-domain is not supported.
- DHCP Snooping with 802.1ah EVCs is not supported.
- B-Bridge and I-Bridge models are not supported.
- An ISID configured under a MAC-Tunnel cannot be configured on another MAC-Tunnel.
- Tunnel-engine configuration is not supported.
- Source MAC address configuration for a Tunnel-Engine is not supported.

### Configuring the MTP for the Cisco 7600 Router

This section describes how to configure MTP for Cisco 7600 Router.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface gigabitEthernet slot/port` or `interface tengigabitEthernet slot/port`
4. `service instance id {Ethernet [service-name]}`
5. `encapsulation untagged dot1q {any | vlan-id[vlan-id][vlan-id]} second-dot1q {any | vlan-id[vlan-id][vlan-id]}`
6. `rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id | 2-to-1 dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} [symmetric]}`
7. `[no] bridge-domain bridge-id c-mac`
8. `exit`
9. `exit`
10. ethernet mac-tunnel virtual mac-in-mac tunnel identifier
11. [no] bridge-domain bridge-id
12. service instance id [Ethernet [service-name]]
13. encapsulation dot1ah i-sid i-sid_number
14. [no] bridge-domain bridge-id c-mac
15. exit
16. exit
17. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface gigabitethernet slot/port</td>
<td>Specifies the Gigabit Ethernet interface to be configured, where: slot/port—Specifies the location of the interface</td>
</tr>
<tr>
<td>Example: Router(config)# interface GigabitEthernet 3/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id Ethernet [service-name]</td>
<td>Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td>Example: Router(config-if)#service instance 20 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation dot1q (any</td>
<td>Configures the encapsulation. Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td>vlan-id[vlan-id[-vlan-id]])) second-dot1q (any</td>
<td></td>
</tr>
<tr>
<td>vlan-id[vlan-id[-vlan-id]]))</td>
<td></td>
</tr>
<tr>
<td>Example: Router(config-if-srv)#encapsulation dot1q 40 second-dot1q 42</td>
<td></td>
</tr>
</tbody>
</table>
802.1ah: Configuring the MAC Tunneling Protocol

Chapter 4      Configuring Layer 1 and Layer 2 Features

### Step 6
**Command:**
```
rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 {dot1q vlan-id dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id}} [symmetric]
```

**Example:**
```
Router(config-if-srv)#rewrite ingress tag pop 1 symmetric
```

**Purpose:** Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.

### Step 7
**Command:** `bridge-domain bd_Id c-mac`

**Example:**
```
Router(config-if-srv)#bridge-domain 21 c-mac
```

**Purpose:** Configuring the bridge domain. Binds the service instance to a bridge domain instance where bd-id is the identifier for the bridge domain instance.

### Step 8
**Command:** `exit`

**Example:**
```
Router(config-if-srv)#exit
```

**Purpose:** Exits the service instance mode.

### Step 9
**Command:** `exit`

**Example:**
```
Router(config-if)#exit
```

**Purpose:** Exits the interface mode.

### Step 10
**Command:** `ethernet mac-tunnel virtual mac-in-mac-TunnelIdentifier`

**Example:**
```
Router(config)#ethernet mac-tunnel virtual 22
```

**Purpose:** Configures mac-in-mac tunnel and creates a tunnel identifier for the 802.1ah cloud. Sets the configuration to config-tunnel-min mode.

### Step 11
**Command:** `bridge-domain bd_Id`

**Example:**
```
Router(config-tunnel-minm)#bridge-domain 200
```

**Purpose:** Binds the MAC tunnel to the B-MAC bridge domain instance.
### Command Purpose

<table>
<thead>
<tr>
<th>Step 12</th>
<th><strong>Command</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>service instance id Ethernet [service-name]</td>
<td>Defines the service instance to be used with B-VLAN. Sets the configuration mode to config-tunnel-srv mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-tunnel-minm)#service instance 23 ethernet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>encapsulation dot1ah i-sid i-sid_number</td>
<td>Defines the matching criteria to be used to map 802.1ah frames with I-SID id to the appropriate EVC.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-tunnel-srv)#encapsulation dot1ah isid 24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>bridge-domain bd_Id c-mac</td>
<td>Maps the I-SID used for forwarding the customer packets to a specific EVC on the interface. To ensure proper configuration, the bd-id used in Step 7 must match the bd-id used in this Step.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-tunnel-srv)#bridge-domain 21 c-mac</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td>Exits the mac-tunnel service instance mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-tunnel-srv)#exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td>Exits the mac-tunnel mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-tunnel-minm)#exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td>Exits the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)#exit</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure MTP for Cisco 7600 Routers:

```
Router>enable
Router#configure terminal
Router(config)#interface GigabitEthernet 3/1
Router(config-if)#service instance 20 ethernet
Router(config-if-srv)#encapsulation dot1q 40 second-dot1q 42
Router(config-if-srv)#rewrite ingress tag pop 1 symmetric
Router(config-if-srv)#bridge-domain 21 c-mac
Router(config-if-srv)#exit
Router(config-if)#exit
Router(config)#ethernet mac-tunnel virtual 22
Router(config-tunnel-minm)#bridge-domain 200
```
802.1ah: Configuring the MAC Tunneling Protocol

Verification

Use the following commands to verify the MTP configuration and view the related information.

- You can use the `show platform mtp slot slot_num` command to verify the MTP configuration and view MTP information for each slot:

```
Router#sh platform mtp slot 3
SLOT TUNNELENGINE VLAN_LIST
  3 MacTunnelEngine3/0 200
  3 MacTunnelEngine3/1
  3 MacTunnelEngine3/2
  3 MacTunnelEngine3/3
```

- You can use `show platform mtp c_bd c-vlan-id` to view information about a specific C-VLAN:

```
Router#sh platform mtp c_bd 21
C_BD B_BD SLOT PPE C_BD_COUNT
  21 200 3 0 1
```

- You can use `show platform mtp b_bd b-vlan-id` to view information about a specific B-VLAN:

```
Router#sh platform mtp b_bd 200
B_BD SLOT PPE B_BD_COUNT
  200 3 0 1
```

- You can use `show platform mtp befp b-efp-id` to view information about a specific B-EFP:

```
Router#sh platform mtp befp 23
BEFP C_BD B_BD SLOT PPE C_BD_COUNT
  23 21 200 3 0 1
```

Troubleshooting

Table 4-36 provides troubleshooting solutions for the MAC Tunnelling feature.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| ethernet mac-tunnel virtual 1 ; bridge-domain 4095 command is rejected | Complete these steps:  
  1. Check the the maximum number of bridge domains you have set.  
  2. Ensure that you have not exceeded the value of 4094. |
| Error message displayed when the I-SID (service identifier) is configured | Complete these steps:  
  1. Check the the maximum number of I-SID you have set.  
  2. Ensure that you have not exceeded the value of 16777215. |
Chapter 4 Configuring Layer 1 and Layer 2 Features

802.3ah: Dying Gasp and Remote Loopback Initiation

Faults in Ethernet connectivity that are caused by slowly deteriorating quality are difficult to detect. Ethernet OAM provides a mechanism for an OAM entity to convey these failure conditions to its peer through specific flags in the OAM PDU. The following failure conditions can be communicated:

- **Link Fault**—Loss of signal is detected by the receiver; for instance, the peer’s laser malfunctions. A link fault is sent once per second in the information OAM PDU. Link fault applies only when the physical sublayer is capable of independently transmitting and receiving signals.
- **Dying Gasp**—An unrecoverable condition occurs; for example, a power failure. This type of condition is vendor specific. A notification about the condition may be sent immediately and continuously.
- **Critical Event**—An unspecified critical event occurs. This type of event is vendor specific. A critical event may be sent immediately and continuously.

In Remote Loopback mode, an OAM entity can put its remote peer into loopback mode using the loopback control OAM PDU. Loopback mode helps an administrator ensure the quality of links during installation or when troubleshooting. In the loopback mode, every frame received is transmitted back on the same port except for OAM PDUs and pause frames. The periodic exchange of OAM PDUs must continue during the loopback state to maintain the OAM session.

**Note**

Effective with Release 15.2(2)S, Dying Gasp and Remote Loopback Initiation is supported on ES+ linecards.

### Restrictions for Dying Gasp and Remote Loopback Initiation

Following restrictions apply for Dying Gasp and Remote Loopback Initiation:

- Internet Group Management Protocol (IGMP) packets are not looped back.
- If dynamic ARP inspection is enabled, ARP or reverse ARP packets are not looped or dropped.
- Control BPDUs like STP, CDP, PAGP, and LACP are not looped back and dropped.
Configuring the Remote Loopback

Complete these steps to enable Ethernet OAM remote loopback on an interface:

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. end
5. ethernet oam remote-loopback start interface type number

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# interface gigabitethernet 1/7</td>
<td></td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Exits the interface and configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5 ethernet oam remote-loopback start interface type number</td>
<td>Starts the loopback initiation.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# ethernet oam remote-loopback start interface gigabitEthernet 1/7</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Dying Gasp

You can configure an error-disable action to occur on an interface if one of the high thresholds is exceeded, if the remote link goes down, if the remote device is rebooted, or if the remote device disables Ethernet OAM on the interface.

Complete these steps to enable Ethernet OAM remote-failure indication actions on an interface:

SUMMARY STEPS

1. enable
2. configure terminal
3. `interface type number`
4. `ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action error-disable-interface`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface type number</code></td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# interface gigabitethernet 1/7</td>
</tr>
<tr>
<td><strong>Step 4</strong> `ethernet oam remote-failure {critical-event</td>
<td>dying-gasp</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# ethernet oam remote-failure dying-gasp action error-disable-interface</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
<td>Exits the interface mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# end</td>
</tr>
</tbody>
</table>

**Configuration Examples**

This example shows how to configure the remote loopback initiation:

```
Router> enable
Router# configure terminal
Router#(config) interface gigabitethernet 1/7
Router(config-if)# end
Router# ethernet oam remote-loopback start interface gigabitEthernet 1/7
```

This example shows how to configure the action on remote-failure reception:

```
Router> enable
Router# configure terminal
Router#(config) interface gigabitethernet 1/7
Router(config-if)# ethernet oam remote-failure dying-gasp action error-disable-interface
```
Verification

This example shows how to verify the configuration:

Router# show ethernet oam status interface gigabitethernet1/7
GigabitEthernet1/7
General
--------
Admin state: enabled
Mode: active
PDU max rate: 10 packets per second
PDU min rate: 1 packet per 1 second
Link timeout: 5 seconds
High threshold action: no action
Link fault action: no action
Dying gasp action: error disable interface
Critical event action: no action

Link Monitoring
---------------
Status: supported (on)
Symbol Period Error
Window: 100 x 1048576 symbols
Low threshold: 1 error symbol(s)
High threshold: none

Frame Error
Window: 10 x 100 milliseconds
Low threshold: 1 error frame(s)
High threshold: none

Frame Period Error
Window: 1000 x 10000 frames
Low threshold: 1 error frame(s)
High threshold: none

Frame Seconds Error
Window: 100 x 100 milliseconds
Low threshold: 1 error second(s)
High threshold: none

Receive-Frame CRC Error
Window: 10 x 100 milliseconds
Low threshold: 10 error frame(s)
High threshold: none

Transmit-Frame CRC Error
Window: 10 x 100 milliseconds
Low threshold: 10 error frame(s)
High threshold: none

This example shows the summary of the remote loopback configuration and the status of the operation:
P19_C7609-S#show ethernet oam summary
Symbols: * - Master Loopback State, # - Slave Loopback State
& - Error Block State
Capability codes: L - Link Monitor, R - Remote Loopback
Support for IEEE 802.1ad

Provider networks handle traffic from a large number of customers. It is important that one customer’s traffic is isolated from the other customer’s traffic. IEEE 802.1ad implements standard protocols for double tagging of data. The data traffic coming from the customer side are double tagged in the provider network where the inner tag is the customer-tag (C-tag) and the outer tag is the provider-tag (S-tag). The control packets are tunneled by changing the destination MAC address in the provider network.

Cisco 7600 series routers already support VLAN double tagging through a feature called QinQ. 802.1ad is the standardized version of QinQ. It also extends the support for Layer 2 Protocol Tunneling Protocol (L2PT). By offering transparent Layer 2 connectivity, the service provider does not get involved in the customer’s Layer 3 network. This makes provisioning and maintenance simple, and reduces the operational cost.

Prerequisites for IEEE 802.1ad

- The ethertype should be programmable per port.

Restrictions for IEEE 802.1ad

Follow these restrictions and guidelines when you configure 802.1ad:

- The `L2protocol forward` command is available only on the main interface of switchports and L3 ports. The command is not available on the subinterfaces. All the subinterfaces on a port inherit the behavior from the main interface. The `L2protocol forward` command is also available on EVC service instance.
- The `L2protocol peer` and `L2protocol drop` commands are not supported.
- The `L2protocol forward` command on a main interface and on EVCs supports only cdp, dtp, vtp, stp, and dot1x.
- You cannot configure Dot1ad if custom ethertype is configured on port.
- 802.1ad is supported on the following port types:

<table>
<thead>
<tr>
<th>Port</th>
<th>EVC</th>
<th>Switchport</th>
<th>Layer Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-UNI</td>
<td>Ethertype 0x8100</td>
<td>Ethertype 0x8100</td>
<td>Ethertype 0x8100</td>
</tr>
<tr>
<td></td>
<td>C-VLAN BPDU</td>
<td>C-VLAN BPDU</td>
<td>C-VLAN BPDU</td>
</tr>
<tr>
<td></td>
<td>Any EVCs</td>
<td>Trunk or Access</td>
<td></td>
</tr>
</tbody>
</table>

Support for IEEE 802.1ad

<table>
<thead>
<tr>
<th>Local Interface</th>
<th>MAC Address</th>
<th>OUI</th>
<th>Mode</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Support for IEEE 802.1ad

Chapter 4 Configuring Layer 1 and Layer 2 Features

Information About IEEE 802.1ad

To configure IEEE 802.1ad support, you should understand the following concepts:

- **How Provider Bridges Work**
- **Guidelines for Handling BPDU**
- **Interoperability of QinQ and Dot1ad**

### How Provider Bridges Work

Provider bridges pass the network traffic of many customers, and each customer's traffic flow must be isolated from one another. For the Layer 2 protocols within customer domains to function properly, geographically separated customer sites must appear to be connected through a LAN, and the provider network must be transparent.

The IEEE has reserved 33 Layer 2 MAC addresses for customer devices operating Layer 2 protocols. If a provider bridge uses these standard MAC addresses for its Layer 2 protocols, the customers' and service provider's Layer 2 traffic will be mixed together. Provider bridges solve this traffic-mixing issue by providing Layer 2 protocol data unit (PDU) tunneling for customers using a provider bridge (S-bridge) component and a provider edge bridge (C-bridge) component. Figure 4-13 shows the topology.

<table>
<thead>
<tr>
<th>Port</th>
<th>EVC</th>
<th>Switchport</th>
<th>Layer Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-UNI</td>
<td>Ethertype 0x88a8</td>
<td>Ethertype 0x88a8</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>S-VLAN BPDU (Only</td>
<td>S-VLAN BPDU</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encapsulation default is supported)</td>
<td>Access only</td>
<td></td>
</tr>
<tr>
<td>S-NNI</td>
<td>Ethertype 0x88a8</td>
<td>Ethertype 0x88a8</td>
<td>S-VLAN BPDU</td>
</tr>
<tr>
<td></td>
<td>S-VLAN BPDU</td>
<td>S-VLAN BPDU</td>
<td>Trunk</td>
</tr>
<tr>
<td></td>
<td>Any EVC</td>
<td>Trunk</td>
<td>Trunk</td>
</tr>
</tbody>
</table>
Support for IEEE 802.1ad

Chapter 4 Configuring Layer 1 and Layer 2 Features

Figure 4-13 Layer 2 PDU Tunneling

S-Bridge Component

The S-bridge component is capable of inserting or removing a service provider VLAN (S-VLAN) for all traffic on a particular port. IEEE 802.1ad adds a new tag called a Service tag (S-tag) to all the ingress frames from a customer to the service provider.

The VLAN in the S-tag is used for forwarding the traffic in the service provider network. Different customers use different S-VLANs, which results in each customer's traffic being isolated. In the S-tag, provider bridges use an Ethertype value that is different from the standard 802.1Q Ethertype value, and do not understand the standard Ethertype. This difference makes customer traffic tagged with the standard Ethertype appear as untagged in the provider network so customer traffic is tunneled in the port VLAN of the provider port. The 802.1ad service provider user network interfaces (S-UNIs) and network to network interfaces (NNIs) implement the S-bridge component.

For example, a VLAN tag has a VLAN ID of 1, the C-tag Ethertype value is 8100 0001, the S-tag Ethertype value is 88A8 0001, and the class of service (CoS) is zero.

C-tag S-tag

| 8100-10 | 8100-20 | 8100-30 |
| 8100-10 | 8100-20 | 8100-30 |

C-Bridge Component

All the C-VLANs entering on a UNI port in an S-bridge component are provided the same service (marked with the same S-VLAN). Although, C-VLAN components are not supported, a customer may want to tag a particular C-VLAN packet separately to differentiate between services. Provider bridges allow C-VLAN packet tagging with a provider edge bridge, called the C-bridge component of the provider bridge. C-bridge components are C-VLAN aware and can insert or remove a C-VLAN 802.1Q tag. The C-bridge UNI port is capable of identifying the customer 802.1Q tag and inserting or removing

| C-Bridge Component |
Support for IEEE 802.1ad

Chapter 4  Configuring Layer 1 and Layer 2 Features

MAC Addresses for Layer 2 Protocols

Customers’ Layer 2 PDUs received by a provider bridge are not forwarded, so Layer 2 protocols running in customer sites do not know the complete network topology. By using a different set of addresses for the Layer 2 protocols running in provider bridges, IEEE 802.1ad causes customers’ Layer 2 PDUs entering the provider bridge to appear as unknown multicast traffic and forwards it on customer ports (on the same S-VLAN). Customers’ Layer 2 protocols can then run transparently.

Table 4-37 shows the Layer 2 MAC addresses reserved for the C-VLAN component.

Table 4-37  Reserved Layer 2 MAC Addresses for a C-VLAN Component

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Group Address</td>
<td>01-80-c2-00-00-00</td>
</tr>
<tr>
<td>IEEE Std 802.3 Full Duplex PAUSE operation</td>
<td>01-80-c2-00-00-01</td>
</tr>
<tr>
<td>IEEE Std. 802.3 Slow Protocols Multicast address</td>
<td>01-80-c2-00-00-02</td>
</tr>
<tr>
<td>IEEE Std. 802.1X PAE address</td>
<td>01-80-c2-00-00-03</td>
</tr>
<tr>
<td>Reserved for future standardization - media access method-specific</td>
<td>01-80-c2-00-00-04</td>
</tr>
<tr>
<td>Reserved for future standardization - media access method-specific</td>
<td>01-80-c2-00-00-05</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-06</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-07</td>
</tr>
<tr>
<td>Provider Bridge Group Address</td>
<td>01-80-c2-00-00-08</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-09</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-0a</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-0b</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-0c</td>
</tr>
<tr>
<td>Provider Bridge GVRP Address</td>
<td>01-80-c2-00-00-0d</td>
</tr>
<tr>
<td>IEEE Std. 802.1AB Link Layer Discovery Protocol multicast address</td>
<td>01-80-c2-00-00-0e</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-0f</td>
</tr>
</tbody>
</table>
Table 4-38 shows the Layer 2 MAC addresses reserved for an S-VLAN component. These addresses are a subset of the C-VLAN component addresses, and the C-bridge does not forward the provider's bridge protocol data units (BPDUs) to a customer network.

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE Std 802.3 Full Duplex PAUSE operation</td>
<td>01-80-c2-00-00-01</td>
</tr>
<tr>
<td>IEEE Std. 802.3 Slow_Protocols_Multicast address</td>
<td>01-80-c2-00-00-02</td>
</tr>
<tr>
<td>IEEE Std. 802.1X PAE address</td>
<td>01-80-c2-00-00-03</td>
</tr>
<tr>
<td>Reserved for future standardization - media access method specific</td>
<td>01-80-c2-00-00-04</td>
</tr>
<tr>
<td>Reserved for future standardization - media access method specific</td>
<td>01-80-c2-00-00-05</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-06</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-07</td>
</tr>
<tr>
<td>Provider Bridge Group Address</td>
<td>01-80-c2-00-00-08</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-09</td>
</tr>
<tr>
<td>Reserved for future standardization</td>
<td>01-80-c2-00-00-0a</td>
</tr>
</tbody>
</table>

Layer 2 Protocol Forwarding Behavior Using EVC Cross-Connect

Table 4-38 shows the Layer 2 BDPU processing for different protocols when using cross-connect for IEEE destination MAC. If tagged, CDP, DTP and VTP packets are forwarded by default using cross-connect configuration.

When Cisco destination MAC is used, all Layer 2 BPDUs (tagged or untagged) are tunneled on S-UNI port and NNI port.

<table>
<thead>
<tr>
<th>IEEE Destination MAC</th>
<th>Protocol</th>
<th>Ethertype/ SNAP Type</th>
<th>EVC - Xconnect Dot1ad uni-C Action</th>
<th>EVC - Xconnect Dot1ad uni-S Action</th>
<th>EVC - Xconnect Dot1ad NNI Action</th>
<th>L2 Protocol Forward Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-00</td>
<td>STP/RSTP/MSTP</td>
<td>Not Applicable</td>
<td>Tunnels, if STP forward is enabled or else peer</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>Yes</td>
</tr>
<tr>
<td>01-80-C2-00-00-01</td>
<td>PAUSE</td>
<td>0x8808</td>
<td>Drops</td>
<td>Drops</td>
<td>Drops</td>
<td>No</td>
</tr>
<tr>
<td>01-80-C2-00-00-02</td>
<td>LACP/LAMP</td>
<td>0x8809/01/02</td>
<td>Tunnels, if L2protocol forward is enabled, or else peer</td>
<td>Tunnels, if L2protocol forward is enabled or else peer</td>
<td>Tunnels, if L2protocol forward is enabled or else peer</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 4-39  Layer 2 Protocol Forwarding Behavior Using EVC Cross-Connect

<table>
<thead>
<tr>
<th>IEEE Destination MAC</th>
<th>Protocol</th>
<th>Ethertype/SNAP Type</th>
<th>EVC - Xconnect Dot1ad uni-C Action</th>
<th>EVC - Xconnect Dot1ad uni-S Action</th>
<th>EVC - Xconnect Dot1ad NNI Action</th>
<th>L2 Protocol Forward Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-02</td>
<td>CDP/DT P/VTP</td>
<td>SNAP type, 2000/03/04</td>
<td>If tagged then tunnels, untagged tunnels if L2protocol forward is enabled or else peers</td>
<td>If tagged then tunnels, untagged tunnels if L2protocol forward is enabled or else peers</td>
<td>If tagged then tunnels, untagged tunnels if L2protocol forward is enabled or else peers</td>
<td>Yes</td>
</tr>
<tr>
<td>01-80-C2-00-00-02</td>
<td>PAGP</td>
<td>SNAP type 0x0104</td>
<td>Tunnels, if L2protocol forward is enabled or else peers</td>
<td>Tunnels, if L2protocol forward is enabled or else peers</td>
<td>Tunnels, if L2protocol forward is enabled or else peers</td>
<td>Yes, enabling forwarding for LACP makes it effective for PAGP also</td>
</tr>
<tr>
<td>01-80-C2-00-00-02</td>
<td>UDLD</td>
<td>SNAP type 0x0111</td>
<td>Peers</td>
<td>Peers</td>
<td>Peers</td>
<td>No</td>
</tr>
<tr>
<td>01-80-C2-00-00-03</td>
<td>802.1X</td>
<td>0x888E</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>No</td>
</tr>
<tr>
<td>01-80-C2-00-00-04</td>
<td>Mac specific control protocol</td>
<td>Not Applicable</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>No</td>
</tr>
<tr>
<td>01-80-C2-00-00-05</td>
<td>Reserved</td>
<td>Not Applicable</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>No</td>
</tr>
<tr>
<td>01-80-C2-00-00-06</td>
<td>Reserved</td>
<td>Not Applicable</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>No</td>
</tr>
<tr>
<td>01-80-C2-00-00-07</td>
<td>ELMI</td>
<td>0x88EE</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>No</td>
</tr>
<tr>
<td>01-80-C2-00-00-08</td>
<td>Provider Bridge Group address</td>
<td>Not Applicable</td>
<td>Drops</td>
<td>Drops</td>
<td>Tunnels, if STP forward is enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>01-80-C2-00-00-09</td>
<td>Reserved</td>
<td>Not Applicable</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>No</td>
</tr>
<tr>
<td>01-80-C2-00-00-0A</td>
<td>Reserved</td>
<td>Not Applicable</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>No</td>
</tr>
<tr>
<td>01-80-C2-00-00-0B</td>
<td>Reserved</td>
<td>Not Applicable</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>No</td>
</tr>
<tr>
<td>01-80-C2-00-00-0C</td>
<td>Reserved</td>
<td>Not Applicable</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>Tunnels</td>
<td>No</td>
</tr>
</tbody>
</table>
Guidelines for Handling BPDU

The general BPDU guidelines are listed here:

UNI-C Ports

The guidelines pertaining to UNI-C ports are:

- VLAN-aware L2 protocols can be peered, tunneled, or dropped.
- Port L2 protocols can either be peered or dropped. They cannot be tunneled.

Table 4-40 shows the Layer 2 PDU destination MAC addresses for customer-facing C-bridge UNI ports, and how frames are processed.

Table 4-40  Layer 2 PDU Destination MAC Addresses for Customer-Facing C-Bridge UNI Ports

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Protocol</th>
<th>Significance on C-UNI Port</th>
<th>Default Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-00</td>
<td>Bridge Group Address (End-to-End BPDUs)</td>
<td>BPDU</td>
<td>Peer</td>
</tr>
<tr>
<td>01-80-C2-00-00-01</td>
<td>802.3X Pause Protocol</td>
<td>BPDU</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-02</td>
<td>Slow Protocol address: 802.3ad LACP, 802.3ah OAM, CDP Pagp, VTP, DTP, UDLD</td>
<td>BPDU</td>
<td>Peer</td>
</tr>
<tr>
<td>01-80-C2-00-00-03</td>
<td>802.1X</td>
<td>BPDU</td>
<td>May peer</td>
</tr>
<tr>
<td>01-80-C2-00-00-04</td>
<td>Reserved for future media access method</td>
<td>None</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-05</td>
<td>Reserved for future media access method</td>
<td>None</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-06</td>
<td>Reserved for future bridge use</td>
<td>None</td>
<td>Drop</td>
</tr>
</tbody>
</table>
### Table 4-40  Layer 2 PDU Destination MAC Addresses for Customer-Facing C-Bridge UNI Ports

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Protocol</th>
<th>Significance on C-UNI Port</th>
<th>Default Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-07</td>
<td>Reserved for future bridge use</td>
<td>None</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-08</td>
<td>Provider STP MAC</td>
<td>None</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-09</td>
<td>Reserved for future bridge use</td>
<td>None</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-0A</td>
<td>Reserved for future bridge use</td>
<td>None</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-0B</td>
<td>Reserved for future S-bridge purpose</td>
<td>None</td>
<td>May peer but not forward</td>
</tr>
<tr>
<td>01-80-C2-00-00-0C</td>
<td>Reserved for future S-bridge purpose</td>
<td>None</td>
<td>May peer but not forward</td>
</tr>
<tr>
<td>01-80-C2-00-00-0D</td>
<td>Provider Bridge GVRP address</td>
<td>None</td>
<td>May peer but not forward</td>
</tr>
<tr>
<td>01-80-C2-00-00-0E</td>
<td>802.1ab-LLDP</td>
<td>BPDU</td>
<td>Peer</td>
</tr>
<tr>
<td>01-80-C2-00-00-0F</td>
<td>Reserved for future C-bridge or Q-bridge use</td>
<td>None</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-10</td>
<td>All bridge addresses</td>
<td>Read Data</td>
<td>May peer</td>
</tr>
<tr>
<td>01-80-C2-00-00-20</td>
<td>GMRP</td>
<td>Data/BPDU</td>
<td>May peer</td>
</tr>
<tr>
<td>01-80-C2-00-00-21</td>
<td>GVRP</td>
<td>Data/BPDU</td>
<td>May peer</td>
</tr>
<tr>
<td>01-80-C2-00-00-22–2F</td>
<td>Other GARP addresses</td>
<td>Data/BPDU</td>
<td>May peer</td>
</tr>
<tr>
<td>01-00-0C-CC-CC-CC</td>
<td>Cisco’s CDP DTP VTP PagP ULDLD</td>
<td>BPDU</td>
<td>Peer</td>
</tr>
<tr>
<td></td>
<td>(End-to-End)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-00-0C-CC-CC-CD</td>
<td>Cisco’s PVST (End-to-End)</td>
<td>BPDU</td>
<td>May peer</td>
</tr>
</tbody>
</table>

**UNI-S Ports**

The guidelines pertaining to UNI-S ports are:

- Packets with C-Bridge addresses (00 - 0F) that are not part of S-Bridge addresses (01 - 0A) are treated as data packet (tunneled).
- VLAN-aware L2 protocols cannot be peered because the port is not C-VLAN aware. They can only be tunneled or dropped.
- Port L2 protocols can be peered, tunneled, or dropped.

**Table 4-41** shows the Layer 2 PDU destination MAC addresses for customer-facing S-bridge UNI ports, and how frames are processed.

### Table 4-41  Layer 2 PDU Destination MAC Addresses for Customer-Facing S-Bridge UNI Ports

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Protocol</th>
<th>Significance on S-UNI Port</th>
<th>Default Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-00</td>
<td>Bridge Group Address (BPDUs)</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>01-80-C2-00-00-01</td>
<td>802.3X Pause Protocol</td>
<td>BPDU</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-02</td>
<td>Slow Protocol address: 802.3ad LACP, 802.3ah</td>
<td>BPDU</td>
<td>Peer</td>
</tr>
</tbody>
</table>
Chapter 4  Configuring Layer 1 and Layer 2 Features

Support for IEEE 802.1ad

Table 4-41  Layer 2 PDU Destination MAC Addresses for Customer-Facing S-Bridge UNI Ports

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Protocol</th>
<th>Significance on S-UNI Port</th>
<th>Default Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-03</td>
<td>802.1X</td>
<td>BPDU</td>
<td>Peer</td>
</tr>
<tr>
<td>01-80-C2-00-00-04</td>
<td>Reserved for future media access method</td>
<td>BPDU</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-05</td>
<td>Reserved for future media access method</td>
<td>BPDU</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-06</td>
<td>Reserved for future bridge use</td>
<td>BPDU</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-07</td>
<td>Reserved for future bridge use</td>
<td>BPDU</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-08</td>
<td>Provider STP (BPDU)</td>
<td>BPDU</td>
<td>Drop (peer on NNI)</td>
</tr>
<tr>
<td>01-80-C2-00-00-09</td>
<td>Reserved for future bridge use</td>
<td>BPDU</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-0A</td>
<td>Reserved for future bridge use</td>
<td>BPDU</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-0B</td>
<td>Reserved for future bridge use</td>
<td>Data if not implemented</td>
<td>Treat as data until implemented</td>
</tr>
<tr>
<td>01-80-C2-00-00-0C</td>
<td>Reserved for future bridge use</td>
<td>Data if not implemented</td>
<td>Treat as data until implemented</td>
</tr>
<tr>
<td>01-80-C2-00-00-0D</td>
<td>Reserved for future GVRP address</td>
<td>Data if not implemented</td>
<td>Treat as data until implemented</td>
</tr>
<tr>
<td>01-80-C2-00-00-0E</td>
<td>802.1ab-LLDP</td>
<td>BPDU</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-0F</td>
<td>Reserved for future C-bridge or Q-bridge use</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>01-80-C2-00-00-10</td>
<td>All bridge addresses</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>01-80-C2-00-00-20</td>
<td>GMRP</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>01-80-C2-00-00-21</td>
<td>GVRP</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>01-80-C2-00-00-22 – 2F</td>
<td>Other GARP addresses</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>01-00-0C-CC-CC-CC</td>
<td>Cisco’s CDP DTP VTP PagP UDLD</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>01-00-0C-CC-CC-CD</td>
<td>Cisco’s PVST</td>
<td>Data</td>
<td>Data</td>
</tr>
</tbody>
</table>

NNI Ports

The Dot1ad NNI ports behave in the same way as the customer facing S-bridge ports, with the following exceptions:

- On NNI ports, frames received with DA 01-80-C2-00-00-08 contain STP BPDU. The frames are received and transmitted. On S-UNI ports, any such frames that are received are dropped, and none are sent.
- On NNI ports, frames received with DA 01-80-C2-00-00-02 include CDP PagP, VTP, DTP, and UDLD protocols.
L2CP Processing According to EPL-1

The restrictions pertaining to Layer 2 control protocol (L2CP) Ethernet Private Line (EPL) service, option 1 (EPL-1) configurations are:

- Supported only on ES+ line cards.
- Dot1ad UNI-S port must be configured before configuring EPL-1.
- L2CP forward must not be configured with EPL options. These may not work together.
- To forward all the L2CP frames by EPL-1 or EPL-2, you must configure the port as a UNI-S port.

The guidelines pertaining to EPL- configurations are:

- EPL-2 option is supported by default.
- Explicit L2CP forward configuration is not required.

Table 4-42 shows the CE2.0 Layer 2 control protocol forwarding requirements for EPL service.

### Table 4-42  CE2.0 Layer 2 Control Protocol Forwarding Requirements for EPL Service

<table>
<thead>
<tr>
<th>Destination MAC</th>
<th>Protocol</th>
<th>Ethertype/Subtype</th>
<th>EPL Option 1</th>
<th>EPL Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-00</td>
<td>STP/RSTP/MSTP</td>
<td></td>
<td>MUST Tunnel</td>
<td>MUST Tunnel</td>
</tr>
<tr>
<td>01-80-C2-00-00-01</td>
<td>PAUSE</td>
<td>0x8808</td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-02</td>
<td>LACP/LAMP</td>
<td>0x8809/01/02</td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-02</td>
<td>Link OAM</td>
<td>0x8809/03</td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-02</td>
<td>ESMC</td>
<td>0x8809/0A</td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-03</td>
<td>802.1X</td>
<td>0x888E</td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-04</td>
<td>Mac specific control protocol</td>
<td></td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-05</td>
<td>Reserved</td>
<td></td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-06</td>
<td>Reserved</td>
<td></td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-07</td>
<td>ELMII</td>
<td>0x88EE</td>
<td>MUST NOT Tunnel</td>
<td>MUST Tunnel</td>
</tr>
<tr>
<td>01-80-C2-00-00-08</td>
<td>Provider Bridge Group address</td>
<td></td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-09</td>
<td>Reserved</td>
<td></td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-0A</td>
<td>Reserved</td>
<td></td>
<td>MUST NOT Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-0B</td>
<td>Reserved</td>
<td></td>
<td>MUST Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-0C</td>
<td>Reserved</td>
<td></td>
<td>MUST Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-0D</td>
<td>Provider Bridge MVRP address</td>
<td></td>
<td>MUST Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-0E</td>
<td>LLDP</td>
<td>0x88CC</td>
<td>MUST NOT Tunnel</td>
<td>MUST Tunnel</td>
</tr>
<tr>
<td>01-80-C2-00-00-0E</td>
<td>PTP Peer delay</td>
<td>0x88F7</td>
<td>MUST NOT Tunnel</td>
<td>MUST Tunnel</td>
</tr>
</tbody>
</table>
Support for IEEE 802.1ad

### Table 4-42  CE2.0 Layer 2 Control Protocol Forwarding Requirements for EPL Service

<table>
<thead>
<tr>
<th>Destination MAC</th>
<th>Protocol</th>
<th>Ethertype/Subtype</th>
<th>EPL Option 1</th>
<th>EPL Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-0F</td>
<td>Reserved</td>
<td></td>
<td>MUST Tunnel</td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-20 through 2F</td>
<td>GARP/GMRP</td>
<td></td>
<td>MUST Tunnel</td>
<td>MUST Tunnel</td>
</tr>
</tbody>
</table>

### 7600 Action Table

Table 4-43 lists the actions performed on a packet when the packet is received with a specified destination MAC address.

**Table 4-43  7600 Action Table**

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Protocol</th>
<th>C-UNI Action</th>
<th>S-UNI Action</th>
<th>NNI Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-00</td>
<td>Bridge Group Address</td>
<td>Peer</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td></td>
<td>(BPDUs)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-01</td>
<td>802.3X Pause Protocol</td>
<td>Drop</td>
<td>Drop</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-02</td>
<td>Slow Protocol address:</td>
<td>Peer</td>
<td>Peer</td>
<td>Peer</td>
</tr>
<tr>
<td></td>
<td>802.3ad LACP, 802.3ah</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-03</td>
<td>802.1X</td>
<td>May peer</td>
<td>May peer</td>
<td>May peer</td>
</tr>
<tr>
<td>01-80-C2-00-00-04</td>
<td>Reserved</td>
<td>Drop</td>
<td>Drop</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-05</td>
<td>Reserved</td>
<td>Drop</td>
<td>Drop</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-06</td>
<td>Reserved</td>
<td>Drop</td>
<td>Drop</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-07</td>
<td>Reserved</td>
<td>Drop</td>
<td>Drop</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-08</td>
<td>Provider STP (BPDU)</td>
<td>Drop</td>
<td>Drop</td>
<td>Peer</td>
</tr>
<tr>
<td>01-80-C2-00-00-09</td>
<td>Reserved for future</td>
<td>Drop</td>
<td>Drop</td>
<td>Drop</td>
</tr>
<tr>
<td></td>
<td>bridge use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-A0</td>
<td>Reserved for future</td>
<td>Drop</td>
<td>Drop</td>
<td>Drop</td>
</tr>
<tr>
<td></td>
<td>bridge use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-0B</td>
<td>Reserved for future</td>
<td>Drop</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td></td>
<td>bridge use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-0C</td>
<td>Reserved for future</td>
<td>Drop</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td></td>
<td>bridge use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-0D</td>
<td>Reserved for future</td>
<td>Drop</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td></td>
<td>GVRP address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-E</td>
<td>802.1ab-LLDP</td>
<td>May peer</td>
<td>Data</td>
<td>Drop</td>
</tr>
<tr>
<td>01-80-C2-00-00-OF</td>
<td>Reserved for future</td>
<td>Drop</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td></td>
<td>C-bridge or Q-bridge use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-10</td>
<td>All bridge addresses</td>
<td>Snoop if</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td></td>
<td>implemented. Else drop</td>
<td>implemented.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-80-C2-00-00-20</td>
<td>GMRP</td>
<td>May peer</td>
<td>Data</td>
<td>Data</td>
</tr>
</tbody>
</table>
Interoperability of QinQ and Dot1ad

The interoperability of QinQ and Dot1ad network enables the exchange of data frames between the networks. The 802.1Q network outer tag VLANs are mapped to the provider S-VLANs of the 802.1ad network.

Figure 4-14 illustrates the interoperability of a Dot1ad network and a QinQ network.

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Protocol</th>
<th>C-UNI Action</th>
<th>S-UNI Action</th>
<th>NNI Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00-21</td>
<td>GVRP</td>
<td>May peer</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>01-80-C2-00-00-22</td>
<td>Other GARP addresses</td>
<td>May peer</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>01-00-0C-CC-CC-CC-CC</td>
<td>Cisco's CDP DTP VTP PagP UDLD</td>
<td>Peer</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>01-00-0C-CC-CC-CC-CD</td>
<td>Cisco’s PVST</td>
<td>May peer</td>
<td>Data</td>
<td>Data</td>
</tr>
</tbody>
</table>

Table 4-43 7600 Action Table

How to Configure IEEE 802.1ad

This section contains the information about following procedures:

- Configuring a Switchport
• Configuring a Layer 2 Protocol Forward
• Configuring a Switchport for Translating QinQ to 802.1ad
• Configuring a Switchport (L2PT)
• Configuring a Customer-Facing UNI-C Port with EVC
• Configuring a Customer-Facing UNI-C Port and Switchport on NNI with EVC
• Configuring a Customer-Facing UNI-S Port with EVC
• Configuring a L2CP Forward Using EPL-1
• Displaying a Dot1ad Configuration

Configuring a Switchport

A switchport can be configured as a UNI-C port, UNI-S port, or NNI port.

UNI-C Port

A UNI-C port can be configured as either a trunk port or an access port. Perform the following tasks to configure a UNI-C port as an access port for 802.1ad.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. ethernet dot1ad {nni | uni {c-port | s-port}}
5. switchport
6. switchport mode {access | trunk}
7. switchport access vlan vlan-id
8. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# interface gigabitethernet 2/1</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 4** ethernet dot1ad \{nni | uni \{c-port | s-port\}\} | Configures a dot1ad NNI port or UNI port. In this example, it is a UNI-C port.
Example:
Router(config-if)# ethernet dot1ad uni c-port

**Step 5** switchport | Put the interface into Layer 2 mode.
Example:
Router(config-if)# switchport

**Step 6** switchport mode \{access | trunk\} | Sets the interface type. In this example, it is Access.
Example:
Router(config-if)# switchport mode access

**Step 7** switchport access vlan vlan-id | Sets the VLAN when an interface is in access mode. In this example, the VLAN is set to 1000.
Example:
Router(config-if)# switchport access 1000

**Step 8** end | Returns the CLI to privileged EXEC mode.
Example:
Router(config-if)# end

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. ethernet dot1ad \{nni | uni \{c-port | s-port\}\}
5. switchport
6. switchport mode \{access | trunk\}
7. switchport trunk allowed vlan vlan-list
8. end

### DETAILED STEPS

| Command or Action | Purpose |
--- | --- |
**Step 1** enable | Enables privileged EXEC mode.
Example:
Router> enable

**Step 2** configure terminal | Enters global configuration mode.
Example:
Router# configure terminal

**Step 3** interface type number | Configures an interface.
Example:
Router# interface gigabitethernet 2/1

Perform the following tasks to configure a UNI-C port as a trunk port for 802.1ad.
UNI-S Port

On a UNI-S port, all the customer VLANs that enter are provided with the same service. The port allows only access configuration. In this mode, the customer’s port is configured as a trunk port. Therefore, the traffic entering the UNI-S port is tagged traffic.

Perform the following tasks to configure a UNI-S port as an access port for 802.1ad.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type number
4. switchport
5. switchport mode {access | trunk}
6. ethernet dot1ad {nni | uni {c-port | s-port}}
7. switchport access vlan vlan-id
8. end

---

**Command or Action** | **Purpose**
--- | ---
Step 4 ethernet dot1ad {nni | uni {c-port | s-port}} | Configures a dot1ad NNI port or UNI port. In this example, it is a UNI-C port.
Example: Router(config-if)# ethernet dot1ad uni c-port
Step 5 switchport | Put the interface into Layer 2 mode.
Example: Router(config-if)# switchport
Step 6 switchport mode {access | trunk} | Sets the interface type. In this example, it is Trunk.
Example: Router(config-if)# switchport mode trunk
Step 7 switchport trunk allowed vlan vlan-list | Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.
Example: Router(config-if)# switchport trunk allowed vlan 1000, 2000
Step 8 end | Returns the CLI to privileged EXEC mode.
Example: Router(config-if)# end

UNI-S Port

On a UNI-S port, all the customer VLANs that enter are provided with the same service. The port allows only access configuration. In this mode, the customer’s port is configured as a trunk port. Therefore, the traffic entering the UNI-S port is tagged traffic.

Perform the following tasks to configure a UNI-S port as an access port for 802.1ad.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type number
4. switchport
5. switchport mode {access | trunk}
6. ethernet dot1ad {nni | uni {c-port | s-port}}
7. switchport access vlan vlan-id
8. end
### Support for IEEE 802.1ad

#### Chapter 4 Configuring Layer 1 and Layer 2 Features

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# interface gigabitethernet 2/1</td>
</tr>
<tr>
<td>Step 4 switchport</td>
<td>Put the interface into Layer 2 mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# switchport</td>
</tr>
<tr>
<td>Step 5 switchport mode {access</td>
<td>trunk}</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# switchport mode access</td>
</tr>
<tr>
<td>Step 6 ethernet dot1ad {nni</td>
<td>uni {c-port</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# ethernet dot1ad uni s-port</td>
</tr>
<tr>
<td>Step 7 switchport access vlan vlan-id</td>
<td>Sets the VLAN when an interface is in access mode. In this example, the VLAN is set to 999.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# switchport access 999</td>
</tr>
<tr>
<td>Step 8 end</td>
<td>Returns the CLI to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# end</td>
</tr>
</tbody>
</table>

**NNI Port**

NNI port allows only trunk configuration. On an NNI port, the frames received on all the allowed VLANs are bridged to the respective internal VLANs.

Perform the following tasks to configure an NNI port as a trunk port for 802.1ad.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type number
4. switchport
5. switchport mode {access | trunk}
6. ethernet dot1ad {nni | uni {c-port | s-port}}
7. switchport trunk allowed vlan vlan-list
8. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Example: enable</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Example: configure terminal</td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router# interface gigabitethernet 2/1</td>
</tr>
<tr>
<td>Router# interface gigabitethernet 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport</td>
<td>Put the interface into Layer 2 mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router(config-if)# switchport</td>
</tr>
<tr>
<td>Router(config-if)# switchport</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport mode {access</td>
<td>trunk}</td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router(config-if)# switchport mode trunk</td>
</tr>
<tr>
<td>Router(config-if)# switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ethernet dot1ad {nni</td>
<td>uni {c-port</td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router(config-if)# ethernet dot1ad nni</td>
</tr>
<tr>
<td>Router(config-if)# ethernet dot1ad nni</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> switchport trunk allowed vlan vlan-list</td>
<td>Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunksing mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router(config-if)# switchport trunk allowed vlan 999</td>
</tr>
<tr>
<td>Router(config-if)# switchport trunk allowed vlan 999</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Returns the CLI to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router(config-if)# end</td>
</tr>
<tr>
<td>Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following example shows how to configure a UNI-C port as an access port. In this example, all the frames that are received are bridged to one internal VLAN 1000. The transmitted frames do not have the access VLAN Dot1q tag.

Router# configure terminal
Router(config)# interface gig2/1
Router(config-if)# ethernet dot1ad uni c-port
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 1000

The following example shows how to configure a UNI-C port as a trunk port. In this example, all the frames that are received on all allowed VLANs (1000 and 2000) are bridged to the respective internal VLANs. The transmitted frames have the respective internal VLAN Dot1q tag.

Router# configure terminal
Router(config)# interface gig2/1
Router(config-if)# ethernet dot1ad uni c-port
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 1000

Delegated to Telcordia
Support for IEEE 802.1ad

Chapter 4  Configuring Layer 1 and Layer 2 Features

The following example shows how to configure a UNI-S port. In this example, all the frames that are received are bridged to one internal VLAN (999). The transmitted frames do not have the access VLAN Dot1q tag.

```
Router# configure terminal
Router(config)# interface gig2/1
Router(config-if)# ethernet dot1ad uni c-port
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# switchport access vlan 1000, 2000
```

The following example shows how to configure an NNI port. Only trunk configuration is allowed on an NNI port. In this example, all the frames that are received on all the allowed VLANs (999) are bridged to the respective internal VLANs. The transmitted frames have the respective internal VLAN Dot1q tag.

```
Router# configure terminal
Router(config)# interface gig2/1
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# ethernet dot1ad uni s-port
Router(config-if)# switchport access vlan 999
```

The following example shows how to configure Dot1ad on an SVI:

```
Router# configure terminal
Router(config)# interface gig2/1
Router(config-if)# ethernet dot1ad nni
Router(config-if)# switchport trunk allowed vlan 999
```

The following example shows how to configure Dot1ad on an SVI:

```
Router# configure terminal
Router(config)# interface gig2/1
Router(config-if)# ethernet dot1ad nni
Router(config-if)# switchport trunk allowed vlan 999
```

Configuring a Layer 2 Protocol Forward

Perform the following tasks to configure the Layer 2 protocol forward:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface` `type number`
4. `switchport access vlan` `vlan-id`
5. `ethernet dot1ad {nni | uni {c-port | s-port}}`
6. `L2protocol [ forward] [protocol]`
7. `end`
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface gigabitethernet 3/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport access vlan vlan-id</td>
<td>Sets the VLAN when an interface is in access mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# switchport access vlan 500</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ethernet dot1ad (nni</td>
<td>uni (c-port</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ethernet dot1ad uni s-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> l2 protocol [forward] protocol</td>
<td>Processes or forwards the Layer 2 BPDUs. In this example, all the BPDUs are forwarded except VTP PDUs.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# l2 protocol forward vtp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Returns the CLI to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

## Examples

The following example shows how to configure a Layer 2 protocol forward:

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/0
Router(config-if)# switchport access vlan 500
Router(config-if)# ethernet dot1ad uni s-port
Router(config-if)# l2 protocol forward vtp
```

## Configuring a Switchport for Translating QinQ to 802.1ad

Translating a QinQ port to 802.1ad involves configuring the port connecting to QinQ port and NNI port. Perform the following tasks to configure a port connecting to the QinQ port.

## SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. switchport mode {access | trunk}
Support for IEEE 802.1ad

Chapter 4  Configuring Layer 1 and Layer 2 Features

5. switchport trunk allowed vlan \textit{vlan-list}
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: \texttt{Router&gt; enable}</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: \texttt{Router# configure terminal}</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface \textit{type number}</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example: \texttt{Router# interface gigabitethernet 1/1}</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport mode {access</td>
<td>trunk}</td>
</tr>
<tr>
<td>Example: \texttt{Router(config-if)# switchport mode trunk}</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport trunk allowed vlan \textit{vlan-list}</td>
<td>Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.</td>
</tr>
<tr>
<td>Example: \texttt{Router(config-if)# switchport trunk allowed vlan 1000}</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns the CLI to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: \texttt{Router(config-if)# end}</td>
<td></td>
</tr>
</tbody>
</table>

Perform the following tasks to configure an NNI port.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface \textit{type number}
4. ethernet dot1ad \{nni | uni \{c-port | s-port\}\}
5. switchport
6. switchport mode \{access | trunk\}
7. switchport trunk allowed vlan \textit{vlan-list}
8. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>interface type number</code></td>
<td>Configures an interface.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>interface gigabitethernet 4/1</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>`ethernet dot1ad {nni</td>
<td>uni {c-port</td>
</tr>
<tr>
<td></td>
<td>Example: <code>ethernet dot1ad nni</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>switchport</code></td>
<td>Put the interface into Layer 2 mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switchport</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`switchport mode {access</td>
<td>trunk}`</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switchport mode trunk</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>switchport trunk allowed vlan vlan-list</code></td>
<td>Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switchport trunk allowed vlan 999-1199</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>end</code></td>
<td>Returns the CLI to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to translate a QinQ port to 802.1ad. In this example, the peer router to gig1/1 multiplexes various customer VLANs into VLAN 1000.

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/1
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk allowed vlan 999-1199
```

```
Router# configure terminal
Router(config)# interface gig4/0
Router(config-if)# ethernet dot1ad nni
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk allowed vlan 1000,1199
```
Configuring a Switchport (L2PT)

Configuring the switchport for L2PT is required to tunnel the STP packets from a customer on the dot1ad network to a customer on the QinQ network.

Perform the following tasks to configure the port connecting to the customer.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. switchport
5. ethernet dot1ad {nni | uni {c-port | s-port}}
6. no l2 protocol [peer | forward] [protocol]
7. L2protocol-tunnel [cdp | stp | vtp]
8. switchport mode {access | trunk}
9. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface gigabitethernet 2/1</td>
<td></td>
</tr>
<tr>
<td>Step 4 switchport</td>
<td>Put the interface into Layer 2 mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# switchport</td>
<td></td>
</tr>
<tr>
<td>Step 5 ethernet dot1ad {nni</td>
<td>uni {c-port</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ethernet dot1ad uni s-port</td>
<td></td>
</tr>
<tr>
<td>Step 6 no l2 protocol [peer</td>
<td>forward] [protocol]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# no l2 protocol forward</td>
<td></td>
</tr>
<tr>
<td>Step 7 L2protocol-tunnel [cdp</td>
<td>stp</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# L2protocol-tunnel stp</td>
<td></td>
</tr>
</tbody>
</table>
Perform the following tasks to configure an NNI port.

### SUMMARY STEPS

1. `enable`  
2. `configure terminal`  
3. `interface type number`  
4. `switchport`  
5. `ethernet dot1ad {nni | uni {c-port | s-port}}`  
6. `switchport mode {access | trunk}`  
7. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface type number</code></td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example: Router(config)# interface gigabitethernet 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>switchport</code></td>
<td>Put the interface into Layer 2 mode.</td>
</tr>
<tr>
<td>Example: Router(config-if)# switchport</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> `ethernet dot1ad {nni</td>
<td>uni {c-port</td>
</tr>
<tr>
<td>Example: Router(config-if)# ethernet dot1ad nni</td>
<td></td>
</tr>
</tbody>
</table>
Support for IEEE 802.1ad

### Chapter 4  Configuring Layer 1 and Layer 2 Features

#### Support for IEEE 802.1ad

**Examples**

The following example shows how to tunnel the STP packets from a customer on the Dot1ad network to a customer on a QinQ network:

```text
Router# configure terminal
Router(config)# interface gig1/0
Router(config-if)# switchport
Router(config-if)# ethernet dot1ad uni s-port
Router(config-if)# no L2protocol forward
Router(config-if)# L2protocol-tunnel stp
Router(config-if)# switchport mode access

Router# configure terminal
Router(config)# interface gig4/0
Router(config-if)# switchport
Router(config-if)# ethernet dot1ad nni
Router(config-if)# switchport mode trunk
```

**Configuring a Customer-Facing UNI-C Port with EVC**

Perform the following tasks to configure a UNI-C port.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ethernet dot1ad {nni | uni {c-port | s-port}}`
5. `service instance id service-type`
6. `encapsulation dot1q vlan-id second-dot1q {any | vlan-id} [native]`
7. `bridge-domain vlan-id`
8. `service instance id service-type`
9. `encapsulation dot1q vlan-id second-dot1q {any | vlan-id} [native]`
10. `bridge-domain vlan-id`
11. `end`

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> `switchport mode (access</td>
<td>trunk)`</td>
</tr>
<tr>
<td>Example: <code>Router(config-if)# switchport mode trunk</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> <code>end</code></td>
<td>Returns the CLI to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Router(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example: Router(config)# interface gigabitethernet 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ethernet dot1ad (nni</td>
<td>uni (c-port</td>
</tr>
<tr>
<td>Example: Router(config-if)# ethernet dot1ad uni c-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> service instance id service-type</td>
<td>Configures an Ethernet service instance. In this example, the service instance is 1.</td>
</tr>
<tr>
<td>Example: Router(config-if)# service instance 1 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> encapsulation dot1q vlan-id second-dot1q (any</td>
<td>vlan-id) [native]</td>
</tr>
<tr>
<td>Example: Router(config-if)# encapsulation dot1q 1-100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> bridge-domain vlan-id</td>
<td>Binds a service instance or a MAC tunnel to a bridge domain.</td>
</tr>
<tr>
<td>Example: Router(config-if)# bridge-domain 1000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> service instance id service-type</td>
<td>Configures an Ethernet service instance. In this example, the service instance is 2.</td>
</tr>
<tr>
<td>Example: Router(config-if)# service instance 2 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> encapsulation dot1q vlan-id second-dot1q (any</td>
<td>vlan-id) [native]</td>
</tr>
<tr>
<td>Example: Router(config-if)# encapsulation dot1q 102-4094</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> bridge-domain vlan-id</td>
<td>Binds a service instance or a MAC tunnel to a bridge domain.</td>
</tr>
<tr>
<td>Example: Router(config-if)# bridge-domain 500</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> end</td>
<td>Returns the CLI to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Perform the following tasks to configure an NNI port.

## SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. ethernet dot1ad {nni | uni {c-port | s-port}}
5. service instance id service-type
6. encapsulation dot1q vlan-id second-dot1q {any | vlan-id} [native]
7. rewrite ingress tag pop 1 symmetric
8. bridge-domain vlan-id
9. service instance id service-type
10. encapsulation dot1q vlan-id second-dot1q {any | vlan-id} [native]
11. rewrite ingress tag pop 1 symmetric
12. bridge-domain vlan-id
13. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface gigabitethernet 2/1</td>
</tr>
<tr>
<td><strong>Step 4</strong> ethernet dot1ad {nni</td>
<td>uni {c-port</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# ethernet dot1ad uni c-port</td>
</tr>
<tr>
<td><strong>Step 5</strong> service instance id service-type</td>
<td>Configures an Ethernet service instance. In this example, the service instance is 1.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# service instance 1 ethernet</td>
</tr>
<tr>
<td><strong>Step 6</strong> encapsulation dot1q vlan-id second-dot1q {any</td>
<td>vlan-id} [native]</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# encapsulation dot1q 1000 second-dot1q 1-100</td>
</tr>
<tr>
<td><strong>Step 7</strong> rewrite ingress tag pop 1 symmetric</td>
<td>Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# rewrite ingress tag pop 1 symmetric</td>
</tr>
</tbody>
</table>
### Command or Action

**Step 8**

**bridge-domain vlan-id**

Example:  
`Router(config-if)# bridge-domain 1000`

**Purpose**

Binds a service instance or a MAC tunnel to a bridge domain.

**Step 9**

**service instance id service-type**

Example:  
`Router(config-if)# service instance 2 ethernet`

**Purpose**

Configures an Ethernet service instance. In this example, the service instance is 2.

**Step 10**

**encapsulation dot1q vlan-id second-dot1q {any | vlan-id} [native]**

Example:  
`Router(config-if)# encapsulation dot1q 500 second-dot1q 102-4904`

**Purpose**

Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.

**Step 11**

**rewrite ingress tag pop 1 symmetric**

Example:  
`Router(config-if)# rewrite ingress tag pop 1 symmetric`

**Purpose**

 Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.

**Step 12**

**bridge-domain vlan-id**

Example:  
`Router(config-if)# bridge-domain 500`

**Purpose**

Binds a service instance or a MAC tunnel to a bridge domain.

**Step 13**

**end**

Example:  
`Router(config-if)# end`

**Purpose**

Returns the CLI to privileged EXEC mode.

### Examples

The following example shows how to configure a customer-facing UNI port. In this example, a dot1q frame coming on VLAN 50 matches service instance 1, and on the ingress port, the rewrite command pushes the 1000 outer-vlan.

```
Router# configure terminal
Router(config)# interface gig1/1
Router(config-if)# ethernet dot1ad uni c-port
Router(config-if)# service instance 1 ethernet
Router(config-if)# encapsulation dot1q 1-100
Router(config-if)# bridge-domain 1000
Router(config-if)# service instance 2 ethernet
Router(config-if)# encapsulation dot1q 102-4904
Router(config-if)# bridge-domain 500
```

```
Router# configure terminal
Router(config)# interface gig4/1
Router(config-if)# ethernet dot1ad nni
Router(config-if)# service instance 1 ethernet
Router(config-if)# encapsulation dot1q 1000 second dot1q 1-100
Router(config-if)# rewrite ingress tag pop 1 symmetric
Router(config-if)# bridge-domain 1000
Router(config-if)# service instance 2 ethernet
Router(config-if)# encapsulation dot1q 500 second dot1q 102-4904
Router(config-if)# rewrite ingress tag pop 1 symmetric
Router(config-if)# bridge-domain 500
```
Configuring a Customer-Facing UNI-C Port and Switchport on NNI with EVC

Perform the following tasks to configure a UNI-C port.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ethernet dot1ad {nni | uni {c-port | s-port}}`
5. `service instance id service-type`
6. `encapsulation dot1q vlan-id second-dot1q {any | vlan-id} [native]`
7. `bridge-domain vlan-id`
8. `service instance id service-type`
9. `encapsulation dot1q vlan-id second-dot1q {any | vlan-id} [native]`
10. `bridge-domain vlan-id`
11. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example: Router(config)# interface gigabitethernet 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ethernet dot1ad {nni</td>
<td>uni {c-port</td>
</tr>
<tr>
<td>Example: Router(config-if)# ethernet dot1ad uni c-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> service instance id service-type</td>
<td>Configures an Ethernet service instance. In this example, the service instance is 1.</td>
</tr>
<tr>
<td>Example: Router(config-if)# service instance 1 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> encapsulation dot1q vlan-id second-dot1q {any</td>
<td>vlan-id} [native]</td>
</tr>
<tr>
<td>Example: Router(config-if)# encapsulation dot1q 1-100</td>
<td></td>
</tr>
</tbody>
</table>
Perform the following tasks to configure an NNI port.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ethernet dot1ad {nni | uni {c-port | s-port}}`
5. `switchport`
6. `switchport mode {access | trunk}`
7. `switchport trunk allowed vlan vlan-list`
8. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code> Router&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Example:</code> Router# <code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 4  Configuring Layer 1 and Layer 2 Features

#### Support for IEEE 802.1ad

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>interface type number</code></td>
<td>Configures an interface.</td>
</tr>
<tr>
<td></td>
<td>Example: Router# interface gigabitethernet 4/1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>`ethernet dot1ad (nni</td>
<td>uni {c-port</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if)# ethernet dot1ad nni</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>switchport</code></td>
<td>Put the interface into Layer 2 mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if)# switchport</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`switchport mode (access</td>
<td>trunk)`</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if)# switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>switchport trunk allowed vlan vlan-list</code></td>
<td>Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if)# switchport trunk allowed vlan 1000-500</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>end</code></td>
<td>Returns the CLI to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure a customer-facing UNI-C port and switchport on NNI with EVC:

```
Router# configure terminal
Router(config)# interface gig1/1
Router(config-if)# ethernet dot1ad uni c-port
Router(config-if)# service instance 1 ethernet
Router(config-if)# encapsulation dot1q 1-100
Router(config-if)# bridge-domain 1000
Router(config-if)# service instance 2 ethernet
Router(config-if)# encapsulation dot1q 102-4904
Router(config-if)# bridge-domain 500
```

```
Router# configure terminal
Router(config)# interface gig4/0
Router(config-if)# switchport
Router(config-if)# ethernet dot1ad uni
Router(config-if)# switchport mode trunk
Router(config-if)# switchport allowed vlan 1000,500
```

### Configuring a Customer-Facing UNI-S Port with EVC

Perform the following tasks to configure a UNI-S port.

---

**Support for IEEE 802.1ad**

Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide

4-318
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. service instance id service-type
5. ethernet dot1ad {nni | uni {c-port | s-port}}
6. encapsulation default
7. bridge-domain vlan-id
8. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface gigabitethernet 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id service-type</td>
<td>Configures an Ethernet service instance. In this example, the service instance is 1.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# service instance 1 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ethernet dot1ad nni uni c-port</td>
<td>Configures a dot1ad NNI port or UNI port. In this example, it is a UNI-S port.</td>
</tr>
<tr>
<td>(c-port</td>
<td>s-port)</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ethernet dot1ad uni s-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> encapsulation default</td>
<td>Configures the default service instance on a port. Anything that does not meet the criteria of other service instances on the same physical interface falls into this service instance.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# encapsulation default</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> bridge-domain vlan-id</td>
<td>Binds a service instance or a MAC tunnel to a bridge domain.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# bridge-domain 1000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Returns the CLI to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Perform the following tasks to configure an NNI port.
### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. service instance id service-type
5. ethernet dot1ad {nni | uni {c-port | s-port}}
6. encapsulation dot1q vlan-id second-dot1q {any | vlan-id} [native]
7. rewrite ingress tag pop 1 symmetric
8. bridge-domain vlan-id
9. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example: Router(config)# interface gigabitethernet 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id service-type</td>
<td>Configures an Ethernet service instance. In this example, the service instance is 1.</td>
</tr>
<tr>
<td>Example: Router(config-if)# service instance 1 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ethernet dot1ad (nni</td>
<td>uni {c-port</td>
</tr>
<tr>
<td>Example: Router(config-if)# ethernet dot1ad uni c-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> encapsulation dot1q vlan-id second-dot1q {any</td>
<td>vlan-id} [native]</td>
</tr>
<tr>
<td>Example: Router(config-if)# encapsulation dot1q 1000 second-dot1q 1-100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> rewrite ingress tag pop 1 symmetric</td>
<td>Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance.</td>
</tr>
<tr>
<td>Example: Router(config-if)# rewrite ingress tag pop 1 symmetric</td>
<td></td>
</tr>
</tbody>
</table>
**Support for IEEE 802.1ad**

### Chapter 4 Configuring Layer 1 and Layer 2 Features

#### Examples

The following example shows how to configure an NNI port:

```
Router# configure terminal
Router(config)# interface gig1/1
Router(config-if)# service instance 1 ethernet
Router(config-if)# ethernet dot1ad nni
Router(config-if)# encapsulation dot1q 1000
Router(config-if)# rewrite ingress tag pop 1 symmetric
Router(config-if)# bridge-domain 1000
```

#### Configuring a L2CP Forward Using EPL-1

To configure L2CP packet processing as per EPL-1, use the `no ethernet l2cp epl-1` command at the interface level.

By default, no form of this command is present and therefore L2CP processing happens according to EPL-2.

Perform the following tasks to configure the L2CP forward using EPL-1:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type number
4. no ip address
5. no keepalive
6. ethernet dot1ad {nni | uni {c-port | s-port}}
7. ethernet l2cp epl-1
8. service instance id ethernet
9. encapsulation default
10. xconnect peer-ip-address vc-id {encapsulation mpls}
11. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface gigabitethernet 5/5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no ip address</td>
<td>Removes an IP address or disables IP processing.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# no ip address</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> no keepalive</td>
<td>Turns off keepalive packets.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# switchport access vlan 500</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ethernet dot1ad (nni</td>
<td>uni (c-port</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ethernet dot1ad uni s-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> ethernet l2cp epl-1</td>
<td>Configure L2CP forward using EPL-1.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ethernet l2cp epl-1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> service instance id ethernet</td>
<td>Creates a service instance on the ethernet interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# service instance 2 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> encapsulation default</td>
<td>Configures the default service instance on a port. Anything that does not meet the criteria of other service instances on the same physical interface falls into this service instance.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if-srv)# encapsulation default</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> xconnect peer-ip-address vc-id (encapsulation mpls)</td>
<td>Binds an attachment circuit to a pseudowire.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if-srv)# xconnect 10.1.1.2 1002 encapsulation mpls</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> end</td>
<td>Returns the CLI to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if-srv)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure a Layer 2 protocol forward:
Configuring a Layer 3 Termination

Perform the following tasks to configure a Layer 3 termination.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ethernet dot1ad {nni | uni {c-port | s-port}}`
5. `interface type number`
6. `encapsulation dot1q vlan-id second-dot1q {any | vlan-id} [native]`
7. `ip address ip-address mask`
8. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code> <code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Example:</code> <code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface type number</code></td>
<td>Configures an interface.</td>
</tr>
<tr>
<td><code>Example:</code> <code>Router(config)# interface gigabitethernet 3/0</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> `ethernet dot1ad {nni</td>
<td>uni {c-port</td>
</tr>
<tr>
<td><code>Example:</code> <code>Router(config-if)# ethernet dot1ad nni</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>interface type number</code></td>
<td>Configures an interface.</td>
</tr>
<tr>
<td><code>Example:</code> <code>Router(config-if)# interface gigabitethernet 3/0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> `encapsulation dot1q vlan-id second-dot1q {any</td>
<td>vlan-id} [native]`</td>
</tr>
<tr>
<td><code>Example:</code> <code>Router(config-if)# encapsulation dot1q 10 second-dot1q 10</code></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4  Configuring Layer 1 and Layer 2 Features

Support for IEEE 802.1ad

Examples

The following example shows how to configure a Layer 3 termination. Note that Layer 3 is supported only on trunk interfaces.

Router# configure terminal
Router(config)# interface gig3/0
Router(config-if)# ethernet dot1ad nni
Router(config)# interface gig3/0/0.1
Router(config-if)# encapsulation dot1q 10 second dot1q 10
Router(config-if)# ip address 1.2.3.4 255.255.0.0

The following example shows how to configure a Layer 3 termination on an SVI:

Router# configure terminal
Router(config)# interface gig4/1
Router(config-if)# ethernet dot1ad nni
Router(config-if)# service instance 1 ethernet
Router(config-if)# encapsulation dot1q 200 second dot1q 300
Router(config-if)# rewrite ingress tag pop 2 symmetric
Router(config-if)# bridge-domain 50
Router(config-if)# service instance 2 ethernet
Router(config-if)# encapsulation dot1q 300
Router(config-if)# rewrite ingress tag pop 1 symmetric
Router(config-if)# bridge-domain 60

Router(config)# interface vlan 50
Router(config-if)# ip address 2.3.4.5 255.255.0.0
Router(config)# interface vlan 60
Router(config-if)# ip address 3.4.5.6 255.255.0.0

Displaying a Dot1ad Configuration

You can display a Dot1ad configuration using the show ethernet dot1ad command. This command displays the Dot1ad configuration for all interfaces. To display the configuration on a particular interface, use the show ethernet dot1ad interface command.

The following example shows how to display a Dot1ad configuration on all interfaces:

Router# show ethernet dot1ad
Interface: GigabitEthernet4/0/1
DOT1AD C-Bridge Port
L2protocol pass cdp stp vtp dtp pagp dot1x lacp

Interface: GigabitEthernet4/0/2
DOT1AD C-Bridge Port
L2protocol pass cdp stp vtp dtp pagp dot1x lacp
Troubleshooting Dot1ad

The following section describes how to troubleshoot Dot1ad.

Note The show commands in these examples should be run from a line card console.

- How do I verify the Dot1ad configuration on a switchport on an X40G card?

  Run the following command to verify the Dot1ad configuration:

  ```
  Router# show platform npc switchport interface gi 1/2
  [GigabitEthernet1/2]
  status [valid, -, applied, enabled]
  src_index [0x1]
  rpcb [0x178BB9C4]
  xlfid [4097]
  xlfid_handle [type:[3] hwidb:[0x20E97F08] if_number:[1121]]
  ft_bits [0x2]
  ing_ctrl_ft_bits [0x2]
  egr_ctrl_ft_bits [0x2]
  port vlan [1]
  mode ingress [NORMAL] egress [NORMAL]
  dot1q_tunnel [No]
  native tagging [No]
  PVLAN isolated or community [No] promiscuous [No]
  ingress vlan-translation [No] BPDU [No]
  egress vlan-translation [No] BPDU [No]
  dot1ad [Yes] <<<<<<<<<<<
  ethertype [0x88A8] <<<<<<<<<<<
  Ingress Stat ID: 778698
  Egress Stat ID: 778700
  VLAN List:
  1
  num of vlans [1]
  Router#
  ```

- How do I verify the Dot1ad configuration on the ports with EVCs on an X40G card?

  Run the following command to verify the Dot1ad configuration:

  ```
  Router# show platform npc xlf interface gi 1/2 efp 1
  EFP XLF(GigabitEthernet1/2, efp1)[np0] = 4136

  Ingress XLF table fields

  Feature common enable: 0x1
  Feature enable: 0x1
  Feature bits: 0x1
  Control common bits: 0x0
  Control feature bits: 0x0
  Control rewrite opcode: 0x0
  Reserved 1: 0x0
  Match cond: 0x1
  Entry valid: 0x1
  Dbus VLAN: 30
  QoS policy ID: 0
  ACL ID: 0
  Statistics ID: 450976
  Inner rewrite VLAN: 0
  Outer rewrite VLAN: 0
  QoS flow ID: 0
  Feature data: 00000000 40000000 AAA80000 E0000829
  ```
Support for IEEE 802.1ad

--- Bridge data -----

layer2_acl_index: 0x00000000
evc_feat_data.ip_src_guard : 0x0
evc_feat_data.mst_evc : 0x1
evc_feat_data.layer2_acl : 0x0
EVC - Mac Security: 0x0
evc_feat_data.sacl : 0x0
evc_feat_data.layer2_acl_statid: 0
PDT: 0xAAA8
ipsg_label: 0
block_data: 0x0
block_l2bpdu: 0x0
split_h: 0x0
imp_ltl: 0x0829

EFP dot1ad port type 0x3

EFP CDP forward 0x1

EFP DTP forward 0x0
EFP VTP forward 0x0
EFP STP forward 0x0
EFP DOT1X forward 0x0

Egress XLIF table fields

Feature common enable: 0x1
Feature enable: 0x1
Feature bits: 0x01
Control common bits: 0x00
Control feature bits: 0x00
Control rewrite opcode: 0x00
Port: 0x1
Match cond 0x1
Entry valid: 0x1
Dbus VLAN: 30
QoS policy ID: 0
ACL ID: 0
Statistics ID: 450980
Inner rewrite VLAN: 0
Outer rewrite VLAN: 0
QoS flow ID: 0
IP Session en : 0
Multicast en : 0
Feature data 0 0x00000000
Intf etype: 0x00008064
Post Filter Opcode 0x00000008
Pre Filter Opcode 0x00000000
Pre Tag Outer 0x00000000
Pre Tag Inner 0x00000000
Post Filter Vlan high 0x00000000
Post Filter Vlan low 0x00000000
Post Filter Vlan outer 0x00000000
EVC - MST: 0x1
EVC etype 0x8100
CFM MEP Level 0x00000008
CFM MIP Level 0x00000008
CFM disable 0x0
MIP filtering 0x0
block_data: 0x0
block_l2bpdu: 0x0
sacl: 0x0
sacl index: 0x0000
sacl statid: 0x000000
Router#
Router#
How do I verify the L2 protocol forwarding on a regular L3 switchports?

Run the following command to verify the L2 protocol forwarding:

```
Router# show platform npc xlif 0 port_sram 1
```

```
dot1ad port type: 0x0002 <<<<<<<<<
l2proto cdp fwd: 0x0001 <<<<<<<<<
12proto dtp fwd: 0x0000
12proto vtp fwd: 0x0000
12proto stp fwd: 0x0000
12proto dotlx fwd: 0x0000
```

How do I verify the Dot1ad configuration on ES20 cards?

For switchports, run the following command:

```
Router# show platform hardware dot1ad l2protocfg port <port-num>
```

For EVCs, run the following command:

```
Router# show platform soft efp-client interface gi x/0/y efp-id l2protocfg
```

To display the default values, run the following commands:

```
Router# show platform hardware dot1ad l2protocfg defaults ?
<0-2> 0=c-uni, 1=s-uni, 2=nni
```

```
Router# show platform hardware dot1ad l2protocfg defaults 0 ?
<0-2> 0=L3, 1=BD, 2=XCON
```

```
Router# show platform hardware dot1ad l2protocfg defaults 0 2
```

```
Raw Data :000FFF77 FFFCFF51
L2 Proto Configs :
Protocol IEEE CISCO
------------------------------------
CDP : FRWD FRWD
VTP : FRWD FRWD
DTP : FRWD FRWD
Others : PEER PEER
802.1d protocols : 01:80:C2:00:00:XX
XX | Config XX | Config XX | Config XX | Config
--------- ------------ -------------- --------------
00 : PEER 01 : DROP 02 : PEER 03 : PEER
04 : FRWD 05 : FRWD 06 : FRWD 07 : FRWD
08 : DROP 09 : FRWD 0A : FRWD 0B : FRWD
0C : FRWD 0D : FRWD 0E : FRWD 0F : FRWD
```

All Bridge (0180C2000010)= FRWD
Group = PEER
PVST = FRWD
How do I verify the L2CP EPL-1 configuration on ES+ line cards?

Run the following command to verify the L2CP EPL-1 configuration:

```
Router# show platform npc xlif 1 port_sram 4
```

Port SRAM fields

```
  hw_frame_type:         0x0001
  hw_dcd_offset:         0x0000
  slot_num:              0x0004
  dbus_ctrl 1:           0x0004
  dbus_ctrl 0:           0x0000
  src_idx 1:             0x0001
  src_idx 0:             0x0004
  enable_tcam:           0x0001
  tcam_profile:          0x0001
  pkt_dir:               0x0000
  ltlbase:               0x0A0
  chnlportbase:          0x0000
  span_session:          0x0000
  bndl_port:             0x0000
  hwidb_vlan:            0x0000
  StormControl Disable:  0x0001
  Multicast StormControl: 0x0000
  Broadcast StormControl: 0x0000
  ethertype_15_8:        0x0088
  ethertype_7_0:         0x00A8
  oam_lb_enable:         0x0
  oam_lb_porttype:       0x0
  MST for xconnect:      0x0
  CRC account:           0x0
  port_block_l2bpdu:     0x0
  port_block_data:       0x0
  mqsos_enable:          0x0000
  mplsogre:              0x0000
  mgre:                  0x0000
  6rd:                   0x0000
  dot1ad port type:      0x0001
  mef epl option:       0x0001 <<<<<<<<<<<<< Set to 1 if EPL-1 is configured, otherwise 0
```

Use the following command to debug L2CP EPL-1 configuration on route processor (RP):

```
Router# debug dot1ad info
```

```
Dot1ad info debugging is on

```
ITU-T G.8032 Ethernet Ring Protection Switching

The G.8032, which is an ethernet ring protection switching (ERPS) feature, provides a protection mechanism, and a protocol for ethernet layer network rings on the Cisco 7600 Series Router platform. This protocol has been standardized by ITU-T. The G.8032 can provide sub-50ms protection and recovery switching for ethernet traffic in a ring topology. This prevents the occurrence of loops that affect the network operation, and the service availability, formed at the ethernet layer. There are two version available for G.8032. G.8032v1 supports a single ring topology while G.8032v2 supports multiple rings or ladder topology.

This chapter provides information about the following topics:
- G.8032 overview, page 4-329
- Restrictions, page 4-332
- Failure Detection, page 4-333
- R-APS Control message Processing, page 4-333
- TCN Processing, page 4-334
- HA/ISSU support, page 4-334
- Configuring the ITU-T G.8032 Feature, page 4-334

G.8032 overview

The G.8032 provides protection switching mechanisms, and a protocol for Ethernet layer network (ETH) rings. Ethernet Rings provide wide-area multipoint connectivity more economically due to less links. The mechanisms and protocol provide reliable and stable protection; and prevents loop formation, which could fatally affect network operation and service availability.

You can prevent loops in an Ethernet Ring by ensuring that, at any moment, traffic may flow on all but one of the ring links, the Ring Protection Link (RPL), where the link is blocked in the working state. When the system detects a link failure, an R-APS Signal Failure (SF) message is multicast to all the nodes, and the failed link end-point ports are blocked. When the RPL owner receives the message, it unblocks the RPL link. The protection switching is triggered, and a new traffic pattern is established on the ring. The blocked ports are then moved to the nodes next to failed ones.

The following functions of G.8032 are supported on the Cisco 7600 Series Router platform:
- Sub-second switching
- EFP bridge-domain over physical or port-channel interfaces
- Up to 32 rings per chassis
- Up to three ERP instances per ring
- Open ring and closed ring support
- Open ring without virtual channel
- G.8032- VPLS TCN Interworking (via LDP MAC Withdrawal)
- G.8032 - REP TCN interworking (TCN propagation)
- G.8032 - G.8032 TCN interworking: TCN propagation from Sub Ring to Major ring
Single Ring Topology

Figure 4-15 shows a 4-node G.8032 single ring topology. The RPL link is between node A and D, and when the network works, the RPL link is blocked by the RPL owner node D and RPL Neighbor Node A.

Figure 4-15  G.8032 Single Ring Topology

Multiple Rings Topology

Figure 4-16 shows two interconnected rings in the multiple rings topology. Ring ERP1 consists of nodes A, B, C and D, and the links between these nodes. Ring ERP2 consists of nodes C, D, E, and F, and the links between C-to-F, F-to-E, and E-to-D. Ring ERP2 on its own does not form a closed loop since the link of C-to-D is owned and controlled by ring ERP1. The closed loop for ring ERP2 can be accomplished by introducing an R-APS virtual channel between the interconnected nodes, C and D, of the sub-ring. R-APS messages of ring ERP2 are encapsulated and transmitted over this virtual channel. If the R-APS virtual channel is not used to close the sub-ring, the R-APS messages are terminated at the interconnected nodes. Blocked ports on all nodes in the ring only block the data traffic, not the R-APS messages to prevent segmentation of the R-APS channel for a non-virtual channel ring implementation. For more information on the ERP in ITU-T G.8032, see: http://www.itu.int/rec/T-REC-G.8032-201003-P/en.
**Figure 4-16  G.8032 Multiple Ring Topology**

**G.8032 Node Components**

Figure 4-17 shows the components for a G.8032 node.

**Figure 4-17  G.8032 Node Components**
ITU-T G.8032 Ethernet Ring Protection Switching

CFM is configured to monitor each ring link, and when CFM detects a link failure, it triggers the ring protection switching. The G.8032 specifications are overlaid on this topology and coordinated by the ERP control module.

As specified by the G.8032 standard, the ERP control module coordinates the information between CFMs received from CFM monitoring and from R-APS messages sent around the ring.

To minimize the packets loss during the switchover, all the relative components in the network need to be High Availability (HA) capable.

Restrictions

These restrictions apply to the G.8032 ERPS:
- G.8032 is only supported on EFP bridge-domains for both physical and port-channel interfaces.
- CFM hardware off loading is not supported on the Cisco 7600 Series Router platform.
- G.8032 is supported only for ES+ line cards (all variants).
- Maximum of 32 rings per box is supported.
- Maximum of 32 ERP instances per ring is supported.
- G.8032 sub-ring with virtual channel is not supported.
- The configuration of Connectivity Fault Management (CFM) for the G.8302 ring requires the setting of a minimum interval of 1 second for the continuity check timer.
Failure Detection

The system could detect these failures:

- LOS Failure: LOS failures are detected by the Cisco 7600 Series Router platform.
- Non-LOS Failure: Non-LOS failures are detected by 802.1ag/Y.1731 CCM in G.8032.

R-APS Control message Processing

ERP uses R-APS Packets to manage and coordinate the protection switching.

R-APS Packet Format

G.8032 R-APS packets are defined in Y.1731 extension (opcode = 40). R-APS packets can be identified by their multicast Destination Media Access Controller (DMAC) + Ethertype DMAC is unique to G.8032; and is shared with Y.1731.

Figure 4-18 shows the G.8032 R-APS control packet format.

Figure 4-18  G.8032 R-APS control packet format

R-APS messages are sent to multicast DMAC. In this feature, the multicast DMAC address is 01-19-A7-00-00-01

CFM and R-APS use the same ethertype (0x8902)

R-APS Packet Transmission Rules

R-APS messages follow the below rules:

9. CPU-originated R-APS packets are forwarded on both ring ports irrespective of blocking status of the R-APS channel.

10. R-APS packets received from a ring (non-CPU-originated) should be punted and also hardware-forwarded to G.8032 network ports. A blocked port drops the hardware-forwarded packets.

11. CPU should not forward the R-APS packets received from ring to G.8032 network ports.

12. R-APS packets received on a blocked port should not be hardware-forwarded, but should be punted to CPU.
13. Exception to rules 2 and 4: In the case of open ring without virtual-channel, the R-APS messages received on a blocked port must be hardware-forwarded on the ring. Therefore, there should be a control knob that is set in the configuration to distinguish this case from the cases of closed ring or open ring with virtual-channel.

**TCN Processing**

Topology changes are notified using TCN, when failures are detected. After receiving TCN from EVC L2 control, Cisco 7600 Series Router platform performs the following operations:

- MAC-Address-Table flush.
- TCN Interworking.

TCN Interworking is needed for:

- G.8032 to VPLS.
- G.8032 sub-Ring to G.8032 Major Ring.
- G.8032 and REP interworking.

**HA/ISSU support**

G.8032 support on the Cisco 7600 Series Router is SSO/ISSU compliant.

**Configuring the ITU-T G.8032 Feature**

See the How to Configure ITU-T G.8032 Ethernet Ring Protection Switching section in the *Carrier Ethernet Configuration Guide, Cisco IOS XE Release 3S*.

**REP Access Gateway EFD**

This feature allows communication for REP to enable Ethernet Fault Detection (EFD) notifications between the Cisco 7600 Series Routers and Cisco ASR 9000 Series Aggregation Services Routers configured with REP Access Gateway (REP-AG).

**Prerequisites for REP Access Gateway**

- The interface connected to non-REP device port should be configured as a REP edge NN port.
- CCM notification is processed only on a REP edge NN port.
- Port MEP is only supported in REP AG.

**Restrictions for REP Access Gateway**

- REP is supported on both EFP and ports; REP AG is supported only for port MEPs.
• When a link down is observed between the REP and Non-REP device, the convergence time is greater with a Copper connection.
• EFD is supported only on physical ports.
• CCM interval for MAs on which EFD is supported is limited.
• EFD is not supported on Trunk EFPs.
• EFD notifications are only supported for a single client per MA. EFD notifications are not supported for both G-8032 and REP simultaneously.
• Only one MEP on a given interface or EFP may be configured for EFD.

Information About REP Access Gateway

In a network when a link failure occurs, a Non-REP device network (access gateway) directly connected to REP network sends failure notification, so that REP network can reroute the traffic to alternate route. But, access devices supporting REP Edge No-Neighbor (REP ENN) only support one interface configured as a REP Edge No-Neighbor port resulting in an unsupported architecture with the REP Access Gateway (REP AG) device.

Fast failure detection can be established by enabling communication between Connectivity Fault Manager (CFM) and REP. CFM on the edge ports can notify REP if any failures are detected on the monitored links, allowing the appropriate re-convergence actions to be taken.

The mechanism for the communication is for REP to register as an Ethernet Fault Detection (EFD) client, so that any CFM defects above a configurable threshold triggers a notification to REP.

Note

To trigger EFD notifications on the router, you must configure CFM.

Configuring the REP Access Gateway Feature

See the How to Configure REP Access Gateway Enhancements section in the LAN Switching Configuration Guide, Cisco IOS XE Release 3S.

Verifying REP Access Gateway

• To display the set of MEPs that have triggered EFD for any client, use this command in service internal mode:

```
Router# show ethernet cfm efd meps
Domain foo, Service bar: notify REP, EFD triggered
  ID Interface SrvcInst Defect        Threshold     Triggered?
  ---- --------- -------- ------------- ------------- ----------
   1   Gi0/0/0      100 DefRDICCM     DefMACstatus  No
  8100   Fa0/0/1      n/a DefXconnCCM   DefMACstatus  Yes

Domain foo, Service blort: notify G.8032, not triggered
```

The output displays the MAs with EFD configured and for each of these MAs, the set of MEPs which have triggered EFD.
Y.1731 Performance Monitoring

When service providers sell connectivity services to a subscriber, a Service Level Agreement (SLA) is reached between the buyer and seller of the service. The SLA defines the attributes offered by a provider and serves as a legal obligation on the service provider. As the level of performance required by subscribers increases, service providers need to monitor the performance parameters being offered. In order to capture the needs of the service providers, organizations have defined various standards such as IEEE 802.1ag and ITU-T Y.1731 that define the methods and frame formats used to measure performance parameters.

Y.1731 Performance Monitoring (PM) provides a standard ethernet PM function that includes measurement of ethernet frame delay, frame delay variation, frame loss, and frame throughput measurements specified by the ITU-T Y.1731 standard and interpreted by the Metro Ethernet Forum (MEF) standards group. As per recommendations, the 7600 platform should be able to send, receive and process PM frames in intervals of 10ms (100 frames per second) with the maximum recommended transmission period being 100ms (10 frames per second) for any given service.

- To display the interface monitored for EFD (CFM CCM) along with the status, use the `show interface number rep detail` command:

  ```
  Router# show interface GigabitEthernet4/0/10 rep detail
  GigabitEthernet4/0/10  REP enabled
  Segment-id: 2 (Preferred Edge No-Neighbor)
  PortID: 030B0015C620BAC0
  Preferred flag: Yes
  Operational Link Status: NO_NEIGHBOR
  Current Key: 0A080007B3A54080EBFE
  Port Role: Open
  Blocked VLAN: <empty>
  Admin-vlan: 1
  Preempt Delay Timer: disabled
  LSL Ageout Timer: 5000 ms
  LSL Ageout Retries: 5
  Configured Load-balancing Block Port: none
  Configured Load-balancing Block VLAN: none
  STCN Propagate to: STP
  EFD State : Enabled <<<<<< If EFD is configured, state is Enabled, else Disabled
  EFD Status : Clear <<<<<< If EFD is configured and no error, status is Clear, else Fault
  LSL PDU rx: 0, tx: 0
  HFL PDU rx: 0, tx: 0
  BPA TLV rx: 0, tx: 0
  BPA (STCN, LSL) TLV rx: 0, tx: 0
  BPA (STCN, HFL) TLV rx: 0, tx: 0
  EPA-ELECTION TLV rx: 0, tx: 10
  EPA-COMMAND TLV rx: 0, tx: 0
  EPA-INFO TLV rx: 0, tx: 0
  ```
To measure SLA parameters such as frame delay or frame delay variation, a small number of synthetic frames are transmitted along with the service to the end point of the maintenance region, where the Maintenance End Point (MEP) responds to the synthetic frame. For a function such as connectivity fault management, the messages are sent less frequently, while performance monitoring frames are sent more frequently.

Figure 4-19 illustrates Maintenance Entities (ME) and Maintenance End Points (MEP) typically involved in a point-to-point metro ethernet deployment for the Y.1731 standard.

Figure 4-19  A point-to-point metro Ethernet deployment with typical Maintenance Entities and Maintenance Points

Following are the performance monitoring parameters:

- Connectivity
- Frame Delay and Frame Delay Variation
- Frame Loss Ratio and Availability

**Connectivity**

The first step to performance monitoring is verifying the connectivity. Continuity Check Messages (CCM) are best suited for connectivity verification, but is optimized for fault recovery operation. It is usually not accepted as a component of an SLA due to the timescale difference between SLA and Fault recovery. Hence, Connectivity Fault Management (CFM) and Continuity Check Database (CCDB) are used to verify connectivity. For more information on CFM see IEEE 802.1ag-2007 Compliant CFM, page 4-237.

**Frame Delay and Frame Delay Variation**

Ethernet frame Delay Measurement (ETH-DM) is used for on-demand ethernet Operations, Administration & Maintenance (OAM) to measure frame delay and frame delay variation.

Ethernet frame delay and frame delay variation are measured by sending periodic frames with ETH-DM information to the peer MEP and receiving frames with ETH-DM information from the peer MEP. During the interval, each MEP measures the frame delay and frame delay variation.
Y.1731 Performance Monitoring

Ethernet frame delay measurement also collects useful information, such as worst and best case delays, average delay, and average delay variation. Ethernet frame delay measurement supports hardware-based timestamping in the ingress direction. It provides a runtime display of delay statistics during a two-way delay measurement. Ethernet frame delay measurement records the last 100 samples collected per remote Maintenance End Point (MEP) or per CFM session.

These are the two methods of delay measurement, as defined by the ITU-T Y.1731 standard:

- **One-way ETH-DM:**
  Each MEP transmits frames with one-way ETH-DM information to its peer MEP in a point-to-point ME to facilitate one-way frame delay and/or one-way frame delay variation measurements at the peer MEP. One way frame delay requires clock to be synchronized at both ends while frame delay variation doesn't require clock synchronization. It is measured using a single delay measurement (1DM) or Delay Measurement Message (DMM) and Delay Measurement Reply (DMR) frame combination.

- **Two-way ETH-DM:**
  Each MEP transmits frames with ETH-DM request information to its peer MEP and receives frames with ETH-DM reply information from its peer MEP. Two way frame delay and frame delay variation is measured using DMM and DMR frame.

These are the pre-requisites for 1DM measurements:

- The clocks of the two concerned end-points must be synchronized accurately and precisely. This is achieved through IEEE 1588-2002.
- There is no auto-session create supported on the peer or the receiver. You need to configure an receive-only session.
- You must configure all the create sessions on the receiver's datapath. These are passive listener sessions.

**Note**

On a Cisco 7600 router, clock synchronization is achieved using a 2-port gigabit synchronous ethernet SPA. On an ES+ line card, the Real Time Clock (RTC) is synchronized to the 2-port gigabit synchronous ethernet SPA time source using Precision Time Protocol (PTP) as the time source protocol. If the time source selected is PTP, all the Y.1731 PM delay packets should have the 1588V2 timestamps.

For a 7600 router that does not have 2-Port Gigabit Synchronous Ethernet SPA, delay measurement is done by using the timestamps with Network Time Protocol (NTP) as the time source protocol. This is applicable only to One-way delay measurements.

To initiate Time of Day (ToD) synchronization on a line card, use the `platform time-source` command in global configuration mode.

Frame Loss Ratio and Availability

Ethernet frame Loss Measurement (ETH-LM) is used to collect counter values applicable for ingress and egress service frames where the counters maintain a count of transmitted and received data frames between a pair of MEPs.

ETH-LM transmits frames with ETH-LM information to a peer MEP and similarly receives frames with ETH-LM information from the peer MEP. Each MEP performs frame loss measurements which contribute to unavailable time. A near-end frame loss refers to frame loss associated with ingress data frames. Far-end frame loss refers to frame loss associated with egress data frames. Both near-end and far-end frame loss measurements contribute to near-end severely errored seconds and far end severely errored seconds which together contribute to unavailable time.

These are the two methods of frame loss measurement, defined by the ITU-T Y.1731 standard:
**Single-ended ETH-LM:** Each MEP transmits frames with the ETH-LM request information to its peer MEP and receives frames with ETH-LM reply information from its peer MEP to carry out loss measurements.

**Dual-ended ETH-LM:** Each MEP transmits periodic dual-ended frames with ETH-LM information to its peer MEP in a point-to-point ME and facilitates frame loss measurements at the peer MEP. As of now, the Cisco 7600 router does not support Dual-ended ETH-LM.

### Y.1731 PM Synthetic Loss Measurement

Synthetic Loss Measurement (SLM) is an extension of the existing Y.1731 PM feature, and makes use of an additional functionality defined in the latest version of the ITU-T Y.1731 (2011) standard. SLM measures frame loss using synthetic frames, rather than data traffic. Frame loss is measured by calculating the difference between the number of synthetic frames that are sent and received.

**Single-ended ETH-SLM**

Single-ended ETH-SLM carries out synthetic loss measurements applicable to both point-to-point ETH connection or multipoint ETH connectivity. The MEP sends frames with the ETH-SLM request information to its peer MEPs and receives frames with ETH-SLM reply information from its peer MEPs to measure synthetic loss.

### Supported Interfaces

Y.1731 PM supports these interfaces:

- LMM, DMM and 1DM support on EVC BD OFM
- LMM, DMM and 1DM support on PC EVC BD OFM
- LMM, DMM and 1DM support on EVC cross-connect OFM
- LMM, DMM and 1DM support on PC EVC cross-connect OFM
- LMM, DMM and 1DM support on EVC cross-connect IFM
- LMM, DMM and 1DM support on PC EVC cross-connect IFM
- LMM, DMM and 1DM support on Subinterfaces (routed port)
- LMM, DMM and 1DM support on PC Subinterfaces (routed port)

**Note**

Release 15.4(1)S onwards, LMM over Port-Channel supports member links on different network processors (NP) and different line cards (LC). This support is available only if fast-switchover is also configured.

### Guidelines and Restrictions for LMM over Port-Channel

- LMM over Port-Channel is supported only if it has two member links in the active-standby mode.
- Member link switchover invalidates the IP SLA session. The session remains invalid till the end of the SLA aggregate interval. The session will resume only at the start of the next aggregate interval.

**Note**

PM is supported in the EVC and CFM configurations mentioned above, with both Dot1q and QinQ encapsulations available on the EVC.
Y.1731 PM SLM supports these interfaces:

- SLM and SLR packet-type support on EVC BD OFM
- SLM and SLR packet-type support on EVC BD IFM
- SLM and SLR packet-type support on PC EVC BD OFM
- SLM and SLR packet-type support on PC EVC BD IFM
- SLM and SLR packet-type support on EVC cross-connect OFM
- SLM and SLR packet-type support on EVC cross-connect IFM
- SLM and SLR packet-type support on PC EVC cross-connect IFM
- SLM and SLR packet-type support on PC EVC cross-connect OFM
- SLM and SLR packet-type support on subinterfaces (routed port)
- SLM and SLR packet-type support on PC subinterfaces (routed port)

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines when you configure Y.1731 PM on an ES+ line card:

- If the route processor CPU is busy with other processes and if software forwarding is used, the performance monitoring statistics are not accurate.
- Y.1731 PM measurement only works for a point to point network topology.
- Y.1731 PM is not SSO compliant. After switchover all sessions data is cleared and IPSLA restart is required.
- In case of one way session or two way session, when one way statistics are required, PTP needs to be synchronized between peers and stable. You should delay starting of sessions in such situations.
- On Cisco 7600 series router, only ES+Line Card is supported in non-switchport mode. PM is not supported on Port MEPs.
- PM is not supported on these interfaces:
  - mLACP interfaces
  - EVC BD IFM
  - Switchport OFM and IFM
  - Port MEPs
- PM is not supported on VPLS configuration.
- PM is not supported on QinQ subinterfaces, as CFM is not supported on these interfaces.
- PM does not support SNMP, although CLI and system-logging is supported.
- Frame Throughput measurements are not supported.

These are the restrictions for PM support on Port-channel:

- Adding or deleting a member link renders the session invalid.
- Loss measurement on port-channel interfaces is supported only if all physical interfaces of the port-channel are present on a single NPU. This restriction cannot be applied for delay measurements.
- All the member links have to be ES+ ports.
- PM is not supported on manual PC EVC Load balancing configuration (UNI LAG).
- CFM Y.1731 packets work with a maximum of two VLAN tags. Expected behavior is not observed with more VLAN tags. CFM Y.1731 packets does not work with untagged cases.

**Note**

Before you begin the Y.1731 PM configurations, ensure that the cfm configurations are up and working. For more information on cfm configurations, please see section IEEE 802.1ag-2007 Compliant CFM, page 4-237

The command `[no] ethernet cfm distribution enable` disables the CFM distribution functionality. This is necessary to avoid performance hits due to the distributing CFM functionality. This command is disabled by default.

## Configuring One Way Delay Measurement

To configure one way delay measurement, complete these steps:

**Note**

Ensure that you first configure a receiver, schedule it to the pending state, and then configure a sender.

### Summary Steps

1. `enable`
2. `configure terminal`
3. `ip sla n`
4. `ethernet y1731 delay receive 1DM domain domain {{vlan | evc} value}cos value {mpid | mac-address} value`
5. `frame {interval | offset | size} value`
6. `history {interval} value`
7. `aggregate {interval} value`
8. `distribution {delay | delay-variation} {one-way | two-way} value`
9. `clock sync`
10. `max-delay value`
11. `owner value`
12. `exit`
13. `ip sla schedule n {life | ageout | recurring | start-time} value start-time start time`
14. `ip sla n`
15. `ethernet y1731 delay 1DM domain domain {{vlan | evc} value} {mpid | mac-address} value cos value source {mpid | mac-address} value`
16. `frame {interval | offset | size} value`
17. `history {interval} value`
18. `aggregate {interval} value`
19. `distribution {delay | delay-variation} {one-way | two-way} value`

20. `clock sync`

21. `max-delay value`

22. `owner value`

23. `exit`

24. `ip sla schedule n {life | ageout | recurring | start-time} value start-time start time`

25. `exit`

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip sla n</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router((config)# ip sla 2</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`ethernet y1731 delay receive 1DM domain domain {{vlan</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`frame {interval</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 6 history (interval) value</td>
<td>Configures Y.1731 history parameters such as:</td>
</tr>
<tr>
<td>Example:</td>
<td>• interval - Specifies the number of intervals. The number of intervals to store ranges between 1 and 10.</td>
</tr>
<tr>
<td>Step 7 aggregate (interval) value</td>
<td>Configures Y.1731 aggregation parameters such as:</td>
</tr>
<tr>
<td>Example:</td>
<td>• interval - Specifies the number of intervals. The aggregation period in seconds ranges between &lt;1-65535&gt;.</td>
</tr>
<tr>
<td>Step 8 distribution (delay</td>
<td>delay-variation) (one-way</td>
</tr>
<tr>
<td>Example:</td>
<td>• delay - Specifies delay distribution parameters.</td>
</tr>
<tr>
<td></td>
<td>• delay-variation - Specifies delay-variation distribution parameters.</td>
</tr>
<tr>
<td></td>
<td>• one-way - Specifies one-way distribution parameters.</td>
</tr>
<tr>
<td></td>
<td>• two-way - Specifies two-way distribution parameters.</td>
</tr>
<tr>
<td>Step 9 clock sync</td>
<td>Checks whether the clocks are synchronized on the sender and receiver.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-sla-y1731-delay)#clock sync</td>
</tr>
<tr>
<td>Step 10 max-delay value</td>
<td>Configures the maximum delay in milliseconds. The value ranges from 1 to 6535.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-sla-y1731-delay)#clock sync</td>
</tr>
<tr>
<td>Step 11 owner value</td>
<td>Specifies the operation owner.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-sla-y1731-delay)#owner name</td>
</tr>
<tr>
<td>Step 12 exit</td>
<td>Exits the Y.1731 submode and enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router((config-sla-y1731-delay)#exit)</td>
</tr>
</tbody>
</table>
### Step 13: `ip sla schedule n (life | ageout | recurring | start-time) value`

Example:
```
Router(config)# ip sla schedule 1 life 100 start-time pending
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Schedules the one way delay measurement on receiver.  
  - `Life` - Specifies a period time to execute in seconds.  
  - `Ageout` - Specifies a period time to keep the entry when inactive.  
  - `Recurring` - Specifies a period time to be scheduled automatically every day.  
  - `Start-time` - Specifies the time to start the entry. The options available are:  
    - `after`
    - `hh:mm`
    - `hh:mm:ss`
    - `now`
    - `pending`

**Note:** On the receiver, the scheduled start time selected should always be pending.

### Step 14: `ip sla n`

Example:
```
Router(config)# ip sla 1
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Enables the IP SLA configuration.

### Step 15: `ethernet y1731 delay 1DM domain domain {vlan | evc | mac-address} value cos value source (mpid | mac-address) value`

Example:
```
Router(config-ip-sla)# ethernet y1731 delay 1DM domain r3 evc e3 mpid 500 cos 3 source mpid 400
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Configures one way delay measurement on sender.  
  - `evc` - Specifies the ethernet virtual circuit identifier.  
  - `vlan` - Specifies the VLAN.  
  - `cos` - Specifies the class of service. The values ranges between 0 and 7.  
  - `mpid` - Specifies the destination MP ID. The values ranges between 1 and 8191.  
  - `mac-address` - Specifies the destination mac-address.  
  - `source` - Specifies the source MP ID or mac-address.

### Step 16: `frame (interval | offset | size) value`

Example:
```
Router(config-sla-y1731-delay)# frame interval 100
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Configures Y.1731 frame parameters such as:  
  - `interval` - Specifies the number of intervals.  
  - `offset` - Specifies the frame offset to be used for calculations. The values ranges between 1 and 10.  
  - `size` - Specifies the frame size. The values ranges between 64 and 384.

### Step 17: `history (interval) value`

Example:
```
Router(config-sla-y1731-delay)# history interval 5
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Configures the Y.1731 history parameters such as:  
  - `interval` - Specifies the number of intervals. The number of intervals to store ranges between 1 and 10.
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 18** aggregate (interval) value | Configures the Y.1731 aggregation parameters such as:  
  - **interval** - Specifies the number of intervals. The aggregation period in seconds ranges between 1 and 65535. |
| Example: Router(config-sla-y1731-delay)# aggregate interval 5 | |
| **Step 19** distribution (delay | delay-variation) (one-way | two-way) value | Configures the Y.1731 distribution parameters such as:  
  - **delay** - Specifies delay distribution parameters.  
  - **delay-variation** - Specifies delay-variation distribution parameters.  
  - **one-way** - Specifies one-way distribution parameters.  
  - **two-way** - Specifies two-way distribution parameters. |
| Example: Router(config-sla-y1731-delay)#distribution delay-variation one-way 2 | |
| **Step 20** clock sync | Checks whether the clocks are synchronized on the sender and receiver. |
| Example: Router(config-sla-y1731-delay)#clock sync | |
| **Step 21** max-delay value | Configures the maximum delay in milliseconds. The value ranges between 1 and 65535. |
| Example: Router(config-sla-y1731-delay)#clock sync | |
| **Step 22** owner value | Specifies the operation owner. |
| Example: Router(config-sla-y1731-delay)#owner name | |
| **Step 23** exit | Exits the Y.1731 submode and enters the global configuration mode. |
| Example: Router((config-sla-y1731-delay)# exit | |
Y.1731 Performance Monitoring

Chapter 4  Configuring Layer 1 and Layer 2 Features

Y.1731 Performance Monitoring

Configuration Example

This example displays the configuration of one way frame delay measurement. Before you begin, configure the receiver, schedule it to pending state, configure the sender and then start the session on it.

Router# enable
Router# configure terminal
On receiver
Router(config)#ip sla 1
Router(config-ip-sla)# ethernet y1731 delay receive 1DM domain r3 evc e3 cos 3 mpid 401
Router(config-sla-y1731-delay)#history interval 5
Router(config-sla-y1731-delay)#aggregate interval 60
Router(config)#exit
Router(config)#ip sla schedule 1 start-time pending

On Sender
Router(config)# ip sla 1
Router(config-ip-sla)# Router(config-ip-sla)# ethernet y1731 delay 1DM domain r3 evc e3 mpid 500 cos 3 source mpid 400
Router(config-sla-y1731-delay)# history interval 5
Router(config-sla-y1731-delay)# aggregate interval 60
Router(config)#exit
Router(config)#ip sla schedule 1 start-time after 00:00:30
Router# end

Configuring Two-Way Delay Measurement

To configure a Two-Way Delay Measurement, complete these steps:

Step 24

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| ip sla schedule n (life | Schedules the one way delay measurement on the sender.
| ageout | • Life - Specifies a period time to be executed in seconds. |
| recurring | • Ageout - Specifies a period time to retain the entry when inactive. |
| start-time value | • Recurring - Specifies the probe to be scheduled automatically every day. |
| start-time start time | • Start-time - Specifies the time to start the entry. The options available are: |

- after
- hh:mm
- hh:mm:ss
- now
- pending

Step 25

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits the global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

Router((config)# exit

Exits the global configuration mode.
Summary Steps

1. enable
2. configure terminal
3. ip sla n
4. ethernet y1731 delay DMM domain domain [{vlan | evc} value] {mpid | mac-address} value cos value source {mpid | mac-address} value
5. frame {interval | offset | size} value
6. history {interval} value
7. aggregate {interval} value
8. distribution {delay | delay-variation} {one-way | two-way} value
9. clock sync
10. max-delay value
11. owner value
12. exit
13. ip sla schedule n {life | ageout | recurring | start-time} value start-time start time
14. end

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>ip sla n</td>
<td>Enables the IP SLA configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# ip sla 1</td>
</tr>
</tbody>
</table>
### Y.1731 Performance Monitoring

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4** | `ethernet y1731 delay DMM domain domain \((\text{vlan} \mid \text{evc}) \text{ value}\) (\text{mpid} \mid \text{mac-address}) \text{ value} \text{ cos value source (mpid} \mid \text{mac-address}) \text{ value}` | Configures a two-way delay measurement on the sender.  
  - `evc` - Specifies the ethernet virtual circuit identifier  
  - `vlan` - Specifies the VLAN.  
  - `cos` - Specifies the class of service. The values ranges between 0 and 7.  
  - `mpid` - Specifies the destination MP ID. The values ranges between 1 and 8191.  
  - `mac-address` - Specifies the destination mac-address.  
  - `source` - Specifies the source MP ID or mac-address. |
| **Step 5** | `frame \((\text{interval} \mid \text{offset} \mid \text{size}) \text{ value}\)` | Configures Y.1731 frame parameters such as:  
  - `interval` - Specifies the number of intervals.  
  - `offset` - Specifies the frame offset to be used for calculations. The values ranges between 1 and 10.  
  - `size` - Specifies the frame size. The values ranges between 64 and 384. |
| **Step 6** | `history \((\text{interval}) \text{ value}\)` | Configures Y.1731 history parameters such as:  
  - `interval` - Specifies the number of intervals. The number of intervals ranges between 1 and 10. |
| **Step 7** | `aggregate \((\text{interval}) \text{ value}\)` | Configures Y.1731 aggregation parameters such as:  
  - `interval` - Specifies the number of intervals. The aggregation period in seconds ranges between 1 and 65535. |
| **Step 8** | `distribution \((\text{delay} \mid \text{delay-variation}) \text{ (one-way} \mid \text{two-way}) \text{ value}\)` | Configures Y.1731 distribution parameters such as:  
  - `delay` - Specifies delay distribution parameters.  
  - `delay-variation` - Specifies delay-variation distribution parameters.  
  - `one-way` - Specifies one-way distribution parameters.  
  - `two-way` - Specifies two-way distribution parameters. |
| **Step 9** | `clock sync` | Checks whether the clocks are synchronized on the sender and receiver. |
The following example configures a two way frame delay measurement.

```
Router# enable
Router# configure terminal
Router(config)# ip sla 1
Router(config-ip-sla)# ethernet y1731-delay DMM domain ifm_400 evc e1 mpid 401 cos 4 source mpid 1
Router(config-sla-y1731-delay)# history interval 5
Router(config-sla-y1731-delay)# aggregate interval 60
Router(config-sla-y1731-delay)# exit
Router(config)# ip sla schedule 1 start-time after 00:00:30
```

**Step 10**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>max-delay value</code></td>
<td>Configures the maximum delay in milliseconds. The value ranges between 1 and 65535.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-sla-y1731-delay)#clock sync</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 11**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>owner value</code></td>
<td>Specifies the operation owner.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-sla-y1731-delay)#owner name</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 12**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits the Y.1731 submode and enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-sla-y1731-delay)#exit</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 13**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ip sla schedule n (life</td>
<td>ageout</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router((config)# ip sla schedule 1 life 100 start-time now</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 14**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router((config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

**Command Purpose**

- **Life** - Specifies the period time to execute in seconds.
- **Ageout** - Specifies the period time to keep the entry when inactive.
- **Recurring** - Specifies the probe to be scheduled automatically every day.
- **Start-time** - Specifies the time to start the entry. The options available are:
  - after
  - hh:mm
  - hh:mm:ss
  - now
  - pending

**Configuration Example**

The following example configures a two way frame delay measurement:

```
Router# enable
Router# configure terminal
Router(config)# ip sla 1
Router(config-ip-sla)# ethernet y1731 delay DMM domain ifm_400 evc e1 mpid 401 cos 4 source mpid 1
Router(config-sla-y1731-delay)# history interval 5
Router(config-sla-y1731-delay)# aggregate interval 60
Router(config-sla-y1731-delay)# exit
Router(config)# ip sla schedule 1 start-time after 00:00:30
```
Configuring Single Ended Frame Loss Measurement

To configure single ended frame loss measurement, complete these steps:

**Note**
Before you begin, configure the command `monitor loss counter [priority cos range]` under the EVC CFM sub-config mode for those interfaces that require loss monitoring.

### Summary Steps

1. enable
2. configure terminal
3. ip sla n
4. ethernet y1731 loss LMM domain domain {vlan | evc} value {mpid | mac-address} value cos value source {mpid | mac-address} value
5. frame {interval | offset | size} value
6. history {interval} value
7. aggregate {interval} value
8. clock sync
9. max-delay value
10. owner value
11. exit
12. ip sla schedule n {life | ageout | recurring | start-time} value start-time start time
13. end

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 4      Configuring Layer 1 and Layer 2 Features

#### Y.1731 Performance Monitoring

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip sla n</code></td>
<td>Enables the IP SLA configuration.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config)# ip sla 1
```

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>`ethernet y1731 loss LMM domain {{(vlan</td>
<td>evc) value}(mpid</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-ip-sla)# ethernet y1731 loss LMM domain r3 evc e3 mpid 500 cos 3 source mpid 400
```

#### Command Purpose

<table>
<thead>
<tr>
<th>Command Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables the IP SLA configuration.</td>
</tr>
<tr>
<td>Configures single ended frame loss measurement on the sender.</td>
</tr>
<tr>
<td>Configures Y.1731 frame parameters such as:</td>
</tr>
<tr>
<td>Configures Y.1731 history parameters such as:</td>
</tr>
<tr>
<td>Configures the Y.1731 aggregation parameters such as:</td>
</tr>
<tr>
<td>Checks whether the clocks are synchronized on the sender and receiver.</td>
</tr>
<tr>
<td>Configures the maximum delay in milliseconds. The value ranges between 1 and 65535.</td>
</tr>
</tbody>
</table>

**Step 5** | `frame (interval | offset | size) value` | Configures Y.1731 frame parameters such as: |

**Example:**

```
Router(config-sla-y1731-loss)# frame interval 100
```

**Step 6** | `history (interval) value` | Configures Y.1731 history parameters such as: |

**Example:**

```
Router(config-sla-y1731-loss)# history interval 5
```

**Step 7** | `aggregate (interval) value` | Configures the Y.1731 aggregation parameters such as: |

**Example:**

```
Router(config-sla-y1731-loss)# aggregate interval 5
```

**Step 8** | `clock sync` | Checks whether the clocks are synchronized on the sender and receiver. |

**Example:**

```
Router(config-sla-y1731-loss)#clock sync
```

**Step 9** | `max-delay value` | Configures the maximum delay in milliseconds. The value ranges between 1 and 65535. |

**Example:**

```
Router(config-sla-y1731-loss)#clock sync
```
Y.1731 Performance Monitoring

**Configuration Example**

This example displays the configuration of single ended frame loss measurement:

```
Router# enable
Router# configure terminal
Router(config)# ip sla 1
Router(config-ip-sla)# ethernet y1731 loss LMM domain r3 vlan 200 mpid 10 cos 3 source
mpid 5
Router(config-sla-y1731-loss)# frame interval 5
Router(config-sla-y1731-loss)# aggregate interval 60
Router(config-sla-y1731-loss)# exit
Router(config)# ip sla schedule 1 life forever start-time now
```

This example displays the configuration of the command `monitor loss counter {priority value}` under the EVC CFM sub-config mode:

```
interface GigabitEthernet3/5
```
no ip address
service instance 1 ethernet e3
encapsulation dot1q 200
bridge-domain 200
cfm mep domain r3 mpid 5
monitor loss counter priority 0-4
!
end

Note
Use the `ip sla reaction-configuration [n] react` command to configure the reaction configuration.

Configuring Single Ended SLM-Continuous

In a Single Ended SLM-Continuous configuration, the frames are transmitted continuously to its peer MEP. To configure single ended SLM-continuous, complete these steps:

Summary Steps

1. enable
2. configure terminal
3. ip sla n
4. ethernet y1731 loss SLM domain domain {{vlan | evc} value} {mpid | mac-address} value cos value source {mpid | mac-address} value
5. history {interval} value
6. aggregate {interval} value
7. exit
8. ip sla schedule n {life | ageout | recurring | start-time} value start-time start time
9. end

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 ip sla n</td>
<td>Enables the IP SLA configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip sla 1</td>
<td></td>
</tr>
</tbody>
</table>
### Step 4

**Command:**

```
ethernet y1731 loss SLM domain
    domain ((vlan | evc) value (mpid | mac-address) value) (mpid | mac-address) value
```

**Example:**

```
Router(config-ip-sla)# ethernet y1731 loss SLM domain CISCO evc PROVIDER mpid 5 cos 4 source mpid 6
```

**Purpose:** Configures single ended synthetic loss measurement-continuous.

- `evc` - Specifies the ethernet virtual circuit identifier.
- `vlan` - Specifies the VLAN.
- `cos` - Specifies the class of service. The values ranges between 0 and 7.
- `mpid` - Specifies the destination MP ID. The values ranges between 1 and 8191.
- `mac-address` - Specifies the destination mac-address.
- `source` - Specifies the source MP ID or mac-address.

### Step 5

**Command:**

```
history interval value
```

**Example:**

```
Router(config-sla-y1731-loss)# history interval 5
```

**Purpose:** Configures Y.1731 history parameters.

- `interval` - Specifies the number of intervals. The number of intervals to store ranges between 1 and 10.

### Step 6

**Command:**

```
aggregate interval value
```

**Example:**

```
Router(config-sla-y1731-loss)# aggregate interval 5
```

**Purpose:** Configures the Y.1731 aggregation parameters.

- `interval` - Specifies the number of intervals. The aggregation period in seconds ranges between 1 and 65535.

### Step 7

**Command:**

```
exit
```

**Example:**

```
Router((config-sla-y1731-loss)# exit
```

**Purpose:** Exits the Y.1731 submode and enters the global configuration mode.
### Chapter 4 Configuring Layer 1 and Layer 2 Features

#### Y.1731 Performance Monitoring

**Configuration Example**

This example shows how to configure the SLM-continuous:

```plaintext
Router# enable
Router# configure terminal
Router(config)# ip sla 1
Router(config-ip-sla)# ethernet y1731 loss SLM domain CISCO evc PROVIDer mpid 10 cos 3
source mpid 5
Router(config-sla-y1731-loss)# history interval 10
Router(config-sla-y1731-loss)# aggregate interval 60
Router(config-sla-y1731-loss)# exit
Router(config)# ip sla schedule 1 life forever start-time now
Router(config)# exit
```

**Step 8**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ip sla schedule n (life</td>
<td>ageout</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# ip sla schedule 1 life 100 start-time now</code></td>
<td></td>
</tr>
</tbody>
</table>

**Notes**

- **Use the `ip sla reaction-configuration [n] react` command to configure the reaction configuration.**
- **Use the `ethernet cfm slm max` command to set the maximum number of SLM receive allowed per box.**
- **Use the `ethernet cfm slm timeout` command to set the idle time for SLM responder entry.**

**Step 9**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 8 Command Purpose**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ip sla schedule n (life</td>
<td>ageout</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# ip sla schedule 1 life 100 start-time now</code></td>
<td></td>
</tr>
</tbody>
</table>

- **Life** - Specifies the time to execute in seconds.
- **Ageout** - Specifies the time to keep the entry when inactive.
- **Recurring** - Specifies automatic scheduling every day.
- **Start-time** - Specifies the time to start the entry. The options available are:
  - `after`
  - `hh:mm`
  - `hh:mm:ss`
  - `now`
  - `pending`
# Configuring Single Ended SLM-Bursts

In a Single Ended SLM-Bursts configuration, the frames are transmitted in bursts to its peer MEP. To configure single ended SLM-Bursts, complete these steps:

## Summary Steps

1. `enable`
2. `configure terminal`
3. `ip sla n`
4. `ethernet y1731 loss SLM burst domain domain {{vlan | evc} value} {mpid | mac-address} value cos value source {mpid | mac-address} value`
5. `history {interval} value`
6. `aggregate {interval} value`
7. `exit`
8. `ip sla schedule n {life | ageout | recurring | start-time} value start-time start time`
9. `end`

## Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip sla n</code></td>
<td>Enables the IP SLA configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# ip sla 1</code></td>
<td></td>
</tr>
</tbody>
</table>
### Y.1731 Performance Monitoring

**Chapter 4      Configuring Layer 1 and Layer 2 Features**

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ethernet y1731 loss SLM burst domain {vlan</td>
<td>evc} value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- evc - Specifies the ethernet virtual circuit identifier.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- vlan - Specifies the VLAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- cos - Specifies the class of service. The values range between 0 and 7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- mpid - Specifies the destination MP ID. The values range between 1 and 8191.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- mac-address - Specifies the destination mac-address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- source - Specifies the source MP ID or mac-address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router(config-ip-sla)# ethernet y1731 loss SLM burst domain CISCO evc PROVIDER mpid 5 cos 4 source mpid 6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>history {interval} value</td>
<td>Configures Y.1731 history parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- interval - Specifies the number of intervals. The number of intervals to store ranges between 1 and 10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router(config-sla-y1731-loss)# history interval 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aggregate {interval} value</td>
<td>Configures the Y.1731 aggregation parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- interval - Specifies the number of intervals. The aggregation period in seconds ranges between 1 and 65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router(config-sla-y1731-loss)# aggregate interval 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Exits the Y.1731 submode and enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router(config-sla-y1731-loss)# exit</td>
</tr>
</tbody>
</table>
Y.1731 Performance Monitoring

Chapter 4 Configuring Layer 1 and Layer 2 Features

### Configuration Example

This example shows how to configure the single ended SLM in bursts:

```plaintext
Router# enable
Router# configure terminal
Router(config)# ip sla 1
Router(config-ip-sla)# ethernet y1731 loss SLM burst domain CISCO evc Provider mpid 10 cos 3 source mpid 5
Router(config-sla-y1731-loss)# history interval 10
Router(config-sla-y1731-loss)# aggregate interval 60
Router(config-sla-y1731-loss)# exit
Router(config)# ip sla schedule 1 life forever start-time now
```

### Verifying the Frame Delay and Frame Loss Measurement Configurations

- To verify and monitor the frame delay and frame delay variation measurement configuration, use this command in privileged EXEC mode:

```plaintext
Router# show ip sla statistics n
```

Delay Statistics for Operation n
Type of operation: Y1731 Delay Measurement
Latest operation start time: *21:37:08.895 PST Thu Aug 20 2009
Latest operation return code:
Distribution Statistics:
Interval <n>
Start time:
Elapsed/End time:
Number of measurements initiated: <x>

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 8** | **ip sla schedule n (life | ageout | recurring | start-time) value**<br>**start-time start time**<br>**Example:**<br>Router((config)# ip sla schedule 1 life 100 start-time now**<br>Schedules the single ended synthetic loss measurement.  
- **Life** - Specifies the length of time to execute in seconds.  
- **Ageout** - Specifies the length of time to keep the entry when inactive.  
- **Recurring** - Specifies automatic scheduling every day.  
- **Start-time** - Specifies the time to start the entry. The options available are:<br>  - after<br>  - hh:mm<br>  - hh:mm:ss<br>  - now<br>  - pending<br>**Step 9** | **exit**<br>**Example:**<br>Router((config)# exit**<br>Exits the global configuration mode.**

---

Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide
Y.1731 Performance Monitoring

Number of measurements completed: <x>
Flag: OK
Delay:
Max/Avg/Min forward: x/y/z  -> Min is only shown if clocks are in sync
Max/Avg/Min backward: x/y/z  -> Only for two-way
Max/Avg/Min: x/y/z  -> Only for two-way
Timestamps backward: Max - xxx/Min - yyy
Timestamps: Max - xxx/Min - yyy
Bucket Forward:
   Bucket Range: 0-9 ms:
      Total observations: <x>
   Bucket Range: 10-19 ms:
      Total observations: <x>
   Bucket Range: 20-29 ms:
      Total observations: <x>
   Bucket Range: 30-39 ms:
      Total observations: <x>
Delay Variance
Max/Avg/Min forward: x/y/z  -> Min is only shown if clocks are in sync
Max/Avg/Min backward: x/y/z  -> Only for two-way
Max/Avg/Min: x/y/z  -> Only for two-way
Bucket Forward:
   Bucket Range: 0-9 ms:
      Total observations: <x>
   Bucket Range: 10-19 ms:
      Total observations: <x>
   Bucket Range: 20-29 ms:
      Total observations: <x>
   Bucket Range: 30-39 ms:
      Total observations: <x>
Operation time to live: Forever

- To verify and monitor the frame loss measurement configuration, use this command in privileged EXEC mode:

   Router# show ip sla statistics n

Delay Statistics for          Operation n
Type of operation: Y1731 Loss Measurement
Latest operation start time: *21:37:08.895 PST Thu Aug 20 2009
Latest operation return code:
Distribution Statistics:
   Interval <n>
   Loss
      Start time:
      Elapsed/End time:
      Number of measurements initiated: <x>
      Number of measurements completed: <x>
      Flag: OK
      Forward
         Tx frame count:
         Rx frame count:
         Available indicators:
         Unavailable indicators:
         Max/Avg/Min(FLR %): 3/2/1
         Max/Avg/Min (FLR Numerator:Denominator)forward: xNum:xDen/yNum:yDen/zNum:zDen
      Backward
         Tx frame count:
         Rx frame count:
         Available indicators:
Unavailable indicators:
Max/Avg/Min (FLR %): 3/2/1
Max/Avg/Min (FLR Numerator:Denominator) backward: xNum:xDen/yNum:yDen/zNum:zDen
Operation time to live: Forever

- To display all details of frame delay and frame delay variation measurements, use the `show ip sla statistics detail` command.

```
Router# show ip sla statistics detail
IPSLAs Latest Operation Statistics
IPSLA operation id: 3
Delay Statistics for Y1731 Operation 3
Type of operation: Y1731 Delay Measurement
Latest operation start time: *00:00:00.000 PST Mon Jan 1 1900
Latest operation return code: OK
Distribution Statistics:
Interval 1
Type: Delay
Start time: *00:00:00.000 PST Mon Jan 1 1900
Elapsed/End time: *00:00:00.000 PST Mon Jan 1 1900
Number of measurements initiated: 0
Number of measurements completed: 0
Flag: OK

Delay:
Max/Avg/Min TwoWay: 140116936/140116944/140116952
Timestamps TwoWay: Max - *00:00:00.000 PST Mon Jan 1 1900/Min - *00:00:00.000 PST Mon Jan 1 1900

Bucket forward:
Bucket Range: 0-4999 microsecond
  Total observations: 0
Bucket Range: 5000-9999 microsecond
  Total observations: 0
Bucket Range: 10000-14999 microsecond
  Total observations: 0
Bucket Range: 15000-19999 microsecond
  Total observations: 0
Bucket Range: 20000-24999 microsecond
  Total observations: 0
Bucket Range: 25000-29999 microsecond
  Total observations: 0
Bucket Range: 30000-34999 microsecond
  Total observations: 0
Bucket Range: 35000-39999 microsecond
  Total observations: 0
Bucket Range: 40000-44999 microsecond
  Total observations: 0
Bucket Range: 45000-50000 microsecond
  Total observations: 0
```

Bucket backward:
Bucket Range: 0-4999 microsecond
  Total observations: 0
Bucket Range: 5000-9999 microsecond
  Total observations: 0
Bucket Range: 10000-14999 microsecond
  Total observations: 0
Bucket Range: 15000-19999 microsecond
  Total observations: 0
Bucket Range: 20000-24999 microsecond
  Total observations: 0
Chapter 4 Configuring Layer 1 and Layer 2 Features

Y.1731 Performance Monitoring

Total observations: 0
Bucket Range: 25000-29999 microsecond
Total observations: 0
Bucket Range: 30000-34999 microsecond
Total observations: 0
Bucket Range: 35000-39999 microsecond
Total observations: 0
Bucket Range: 40000-44999 microsecond
Total observations: 0
Bucket Range: 45000--2 microsecond
Total observations: 0

Bucket TwoWay:
Bucket Range: 0-0 microsecond
Total observations: 0
Bucket Range: 1-1 microsecond
Total observations: 0
Bucket Range: 2-2 microsecond
Total observations: 0
Bucket Range: 3-3 microsecond
Total observations: 0
Bucket Range: 4--2 microsecond
Total observations: 0

Delay Variance:
Max/Avg backward positive: 140116936/140116944
Timestamp backward positive: Max - *00:00:00.000 PST Mon Jan 1 1900
Max/Avg backward negative: 140116936/140116944
Timestamp backward negative: Max - *00:00:00.000 PST Mon Jan 1 1900
Max/Avg TwoWay positive: 140116936/140116944
Timestamp TwoWay positive: Max - *00:00:00.000 PST Mon Jan 1 1900
Max/Avg TwoWay negative: 140116936/140116944
Timestamp TwoWay negative: Max - *00:00:00.000 PST Mon Jan 1 1900

Bucket forward positive:
Bucket Range: 0-4999 microsecond
Total observations: 0
Bucket Range: 5000-9999 microsecond
Total observations: 0
Bucket Range: 10000-14999 microsecond
Total observations: 0
Bucket Range: 15000-19999 microsecond
Total observations: 0
Bucket Range: 20000-24999 microsecond
Total observations: 0
Bucket Range: 25000-29999 microsecond
Total observations: 0
Bucket Range: 30000-34999 microsecond
Total observations: 0
Bucket Range: 35000-39999 microsecond
Total observations: 0
Bucket Range: 40000-44999 microsecond
Total observations: 0
Bucket Range: 45000--2 microsecond
Total observations: 0

Bucket forward negative:
Bucket Range: 0-4999 microsecond
Total observations: 0
Bucket Range: 5000-9999 microsecond
Total observations: 0
Bucket Range: 10000-14999 microsecond
Total observations: 0
Bucket Range: 15000-19999 microsecond
Total observations: 0
Bucket Range: 20000-24999 microsecond
Total observations: 0
Bucket Range: 25000-29999 microsecond
Total observations: 0
Bucket Range: 30000-34999 microsecond
Total observations: 0
Bucket Range: 35000-39999 microsecond
Total observations: 0
Bucket Range: 40000-44999 microsecond
Total observations: 0
Bucket Range: 45000--2 microsecond
Total observations: 0
Y.1731 Performance Monitoring

Bucket Range: 15000-19999 microsecond
Total observations: 0
Bucket Range: 20000-24999 microsecond
Total observations: 0
Bucket Range: 25000-29999 microsecond
Total observations: 0
Bucket Range: 30000-34999 microsecond
Total observations: 0
Bucket Range: 35000-39999 microsecond
Total observations: 0
Bucket Range: 40000-44999 microsecond
Total observations: 0
Bucket Range: 45000-49999 microsecond
Total observations: 0

Bucket backward positive:
Bucket Range: 0-4999 microsecond
Total observations: 0
Bucket Range: 5000-9999 microsecond
Total observations: 0
Bucket Range: 10000-14999 microsecond
Total observations: 0
Bucket Range: 15000-19999 microsecond
Total observations: 0
Bucket Range: 20000-24999 microsecond
Total observations: 0
Bucket Range: 25000-29999 microsecond
Total observations: 0
Bucket Range: 30000-34999 microsecond
Total observations: 0
Bucket Range: 35000-39999 microsecond
Total observations: 0
Bucket Range: 40000-44999 microsecond
Total observations: 0
Bucket Range: 45000-49999 microsecond
Total observations: 0

Bucket backward negative:
Bucket Range: 0-4999 microsecond
Total observations: 0
Bucket Range: 5000-9999 microsecond
Total observations: 0
Bucket Range: 10000-14999 microsecond
Total observations: 0
Bucket Range: 15000-19999 microsecond
Total observations: 0
Bucket Range: 20000-24999 microsecond
Total observations: 0
Bucket Range: 25000-29999 microsecond
Total observations: 0
Bucket Range: 30000-34999 microsecond
Total observations: 0
Bucket Range: 35000-39999 microsecond
Total observations: 0
Bucket Range: 40000-44999 microsecond
Total observations: 0
Bucket Range: 45000-49999 microsecond
Total observations: 0

Bucket TwoWay positive:
Bucket Range: 0-4999 microsecond
Total observations: 0
Bucket Range: 5000-9999 microsecond
Total observations: 0
Bucket Range: 10000-14999 microsecond
Total observations: 0
Bucket Range: 15000-19999 microsecond
Total observations: 0
Bucket Range: 20000-24999 microsecond
Total observations: 0
Bucket Range: 25000-29999 microsecond
Total observations: 0
Bucket Range: 30000-34999 microsecond
Total observations: 0
Bucket Range: 35000-39999 microsecond
Total observations: 0
Bucket Range: 40000-44999 microsecond
Total observations: 0
Bucket Range: 45000-2 microsecond
Total observations: 0

- To display the same outputs as the latest statistics detail command, use the `show ip sla history interval n` command. The number displayed is the number of intervals configured.

### Output for Loss Measurement:

```
Router# show ip sla history 1 interval-statistics
Loss Statistics for Y1731 Operation 1
Type of operation: Y1731 Loss Measurement
Latest operation start time: *09:46:16.225 UTC Fri Nov 26 2010
Latest operation return code: OK
Distribution Statistics:

Interval 1
Start time: *09:46:16.225 UTC Fri Nov 26 2010
End time:  *09:48:16.221 UTC Fri Nov 26 2010
Number of measurements initiated: 12006
Number of measurements completed: 12000
Flag: OK

Forward
Number of Observations 11999
Timestamps forward:
Tx frame count: 30000
Rx frame count: 20000
Available indicators: 11999
Unavailable indicators: 0
Max/Avg/Min - (FLR % ): 1:3/2.78%/0:0

Backward
Number of Observations 11999
Timestamps backward:
Tx frame count: 10000
Rx frame count: 10000
Available indicators: 11999
Unavailable indicators: 0
Max/Avg/Min - (FLR % ): 0:0/0.0%/0:0
```

### Output for Delay Measurement:

```
Router# show ip sla history 10 interval-statistics
Delay Statistics for Y1731 Operation 10
Type of operation: Y1731 Delay Measurement
Latest operation start time: 10:58:30.144 PDT Tue Jan 4 2011
Latest operation return code: Timeout
Distribution Statistics:
```
Y.1731 Performance Monitoring

Interval 1
Start time: 10:58:30.144 PDT Tue Jan 4 2011
End time: 10:59:05.140 PDT Tue Jan 4 2011
Number of measurements initiated: 33
Number of measurements completed: 34
Flag: OK

Delay:
Number of TwoWay observations: 34
Max/Avg/Min TwoWay: 113364/100499/100099 (microsec)
Time of occurrence TwoWay:
Max – 10:59:05.140 PDT Tue Jan 4 2011
Min – 10:58:40.076 PDT Tue Jan 4 2011

Bin TwoWay:

<table>
<thead>
<tr>
<th>Bin Range (microsec)</th>
<th>Total observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 – &lt; 5000</td>
<td>0</td>
</tr>
<tr>
<td>5000 – &lt; 10000</td>
<td>0</td>
</tr>
<tr>
<td>10000 – &lt; 15000</td>
<td>0</td>
</tr>
<tr>
<td>15000 – &lt; 20000</td>
<td>0</td>
</tr>
<tr>
<td>20000 – &lt; 25000</td>
<td>0</td>
</tr>
<tr>
<td>25000 – &lt; 30000</td>
<td>0</td>
</tr>
<tr>
<td>30000 – &lt; 35000</td>
<td>0</td>
</tr>
<tr>
<td>35000 – &lt; 40000</td>
<td>0</td>
</tr>
<tr>
<td>40000 – &lt; 45000</td>
<td>0</td>
</tr>
<tr>
<td>45000 – &lt; 4294967295</td>
<td>34</td>
</tr>
</tbody>
</table>

Delay Variance:
Number of TwoWay positive observations: 19
Max/Avg TwoWay positive: 13256/706 (microsec)
Time of occurrence TwoWay positive:
Max – 10:59:05.140 PDT Tue Jan 4 2011

Number of TwoWay negative observations: 14
Max/Avg TwoWay negative: 86/11 (microsec)
Time of occurrence TwoWay negative:
Max – 10:58:40.076 PDT Tue Jan 4 2011

Bin TwoWay positive:

<table>
<thead>
<tr>
<th>Bin Range (microsec)</th>
<th>Total observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 – &lt; 5000</td>
<td>18</td>
</tr>
<tr>
<td>5000 – &lt; 10000</td>
<td>0</td>
</tr>
<tr>
<td>10000 – &lt; 15000</td>
<td>1</td>
</tr>
<tr>
<td>15000 – &lt; 20000</td>
<td>0</td>
</tr>
<tr>
<td>20000 – &lt; 25000</td>
<td>0</td>
</tr>
<tr>
<td>25000 – &lt; 30000</td>
<td>0</td>
</tr>
<tr>
<td>30000 – &lt; 35000</td>
<td>0</td>
</tr>
<tr>
<td>35000 – &lt; 40000</td>
<td>0</td>
</tr>
<tr>
<td>40000 – &lt; 45000</td>
<td>0</td>
</tr>
<tr>
<td>45000 – &lt; 4294967295</td>
<td>0</td>
</tr>
</tbody>
</table>

Bin TwoWay negative:

<table>
<thead>
<tr>
<th>Bin Range (microsec)</th>
<th>Total observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 – &lt; 5000</td>
<td>14</td>
</tr>
<tr>
<td>5000 – &lt; 10000</td>
<td>0</td>
</tr>
<tr>
<td>10000 – &lt; 15000</td>
<td>0</td>
</tr>
<tr>
<td>15000 – &lt; 20000</td>
<td>0</td>
</tr>
<tr>
<td>20000 – &lt; 25000</td>
<td>0</td>
</tr>
<tr>
<td>25000 – &lt; 30000</td>
<td>0</td>
</tr>
<tr>
<td>30000 – &lt; 35000</td>
<td>0</td>
</tr>
<tr>
<td>35000 – &lt; 40000</td>
<td>0</td>
</tr>
<tr>
<td>40000 – &lt; 45000</td>
<td>0</td>
</tr>
<tr>
<td>45000 – &lt; 4294967295</td>
<td>0</td>
</tr>
</tbody>
</table>
Chapter 4      Configuring Layer 1 and Layer 2 Features

Y.1731 Performance Monitoring

- To display the performance monitoring session summary, use the `show ethernet cfm pm session summary` command.

Router# show ethernet cfm pm session summary
Number of Configured Session : 1
Number of Active Session: 1
Number of Inactive Session: 0

- To verify and monitor the Single Ended Synthetic Loss Measurement configuration, use these commands in privileged EXEC mode:

  - `show ip sla statistics entry-number`

Router# show ip sla statistics 100
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
Loss Statistics for Y1731 Operation 100
Type of operation: Y1731 Loss Measurement
Latest operation start time: *03:59:48.036 UTC Mon Oct 1 2012
Latest operation return code: OK
Distribution Statistics:

Interval
Start time:  *03:59:48.036 UTC Mon Oct 1 2012
Elapsed time: 48 seconds
Number of measurements initiated: 24
Number of measurements completed: 23
Flag: OK

  - `show ip sla statistics details`

Router# show ip sla stat details
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
Loss Statistics for Y1731 Operation 100
Type of operation: Y1731 Loss Measurement
Latest operation start time: *03:59:48.036 UTC Mon Oct 1 2012
Latest operation return code: OK
Distribution Statistics:

Interval
Start time:  *03:59:48.036 UTC Mon Oct 1 2012
Elapsed time: 56 seconds
Number of measurements initiated: 53
Number of measurements completed: 52
Flag: OK

Forward
Number of Observations 5
Available indicators: 0
Unavailable indicators: 5
Tx frame count: 50
Rx frame count: 50
  Min/Avg/Max - (FLR %): 0:9/000.00%/0:9
Cumulative - (FLR %): 000.0000%
Timestamps forward:
  Min - *04:00:37.807 UTC Mon Oct 1 2012
  Max - *04:00:37.807 UTC Mon Oct 1 2012

Backward
Number of Observations 5
Y.1731 Performance Monitoring

Chapter 4 Configuring Layer 1 and Layer 2 Features

Y.1731 Performance Monitoring

Available indicators: 0
Unavailable indicators: 5
Tx frame count: 50
Rx frame count: 49
Min/Avg/Max - (FLR %): 0:9/000.00%/0:9
Cumulative - (FLR %): 002.0000%
Timestamps backward:
Min - *04:00:37.807 UTC Mon Oct 1 2012
Max - *04:00:37.807 UTC Mon Oct 1 2012

```
show ip sla statistics aggregated entry-number
```

```
Router# show ip sla statistics aggregated 100
IPSLAs aggregated statistics

IPSLA operation id: 100
Loss Statistics for Y1731 Operation 100
Type of operation: Y1731 Loss Measurement
Latest operation start time: *03:59:48.036 UTC Mon Oct 1 2012
Latest operation return code: OK
Distribution Statistics:

Interval
Start time:   *03:59:48.036 UTC Mon Oct 1 2012
Elapsed time: 68 seconds
Number of measurements initiated: 53
Number of measurements completed: 52
Flag: OK

Forward
Number of Observations 5
Available indicators: 0
Unavailable indicators: 5
Tx frame count: 50
Rx frame count: 50
Min/Avg/Max - (FLR %): 0:9/000.00%/0:9
Cumulative - (FLR %): 000.0000%
Timestamps forward:
Min - *04:00:37.807 UTC Mon Oct 1 2012
Max - *04:00:37.807 UTC Mon Oct 1 2012

Backward
Number of Observations 5
Available indicators: 0
Unavailable indicators: 5
Tx frame count: 50
Rx frame count: 49
Min/Avg/Max - (FLR %): 0:9/000.00%/0:9
Cumulative - (FLR %): 002.0000%
Timestamps backward:
Min - *04:00:37.807 UTC Mon Oct 1 2012
Max - *04:00:37.807 UTC Mon Oct 1 2012

```
– show ip sla statistics aggregated entry-number details
```

```
Router# show ip sla statistics aggregated 100 details
IPSLAs aggregated statistics

IPSLA operation id: 100
Loss Statistics for Y1731 Operation 100
Type of operation: Y1731 Loss Measurement
Latest operation start time: *03:59:48.036 UTC Mon Oct 1 2012
Latest operation return code: OK
Distribution Statistics:

```
Y.1731 Performance Monitoring

Interval
Start time: 03:59:48.036 UTC Mon Oct 1 2012
Elapsed time: 118 seconds
Number of measurements initiated: 112
Number of measurements completed: 111
Flag: OK

Forward
Number of Observations 11
Available indicators: 11
Unavailable indicators: 0
Tx frame count: 110
Rx frame count: 110
Min/Avg/Max - (FLR %): 0.9/0.9/0.9
Cumulative - (FLR %): 000.000%
Timestamps forward:
Min - 04:01:39.201 UTC Mon Oct 1 2012
Max - 04:01:39.201 UTC Mon Oct 1 2012

Backward
Number of Observations 11
Available indicators: 11
Unavailable indicators: 0
Tx frame count: 110
Rx frame count: 109
Min/Avg/Max - (FLR %): 0.9/0.9/0.9
Cumulative - (FLR %): 000.009%
Timestamps backward:
Min - 04:01:39.201 UTC Mon Oct 1 2012
Max - 04:01:39.201 UTC Mon Oct 1 2012

To display the performance monitoring sessions for Y.1731 PM SLM, use these commands:

- show ethernet cfm pm session active

Router# show ethernet cfm pm session active
Display of Active Session
------------------------------------------
<table>
<thead>
<tr>
<th>EPM-ID</th>
<th>SLA-ID</th>
<th>Lvl/Type/ID/Cos/Dir</th>
<th>Src-Mac-address</th>
<th>Dst-Mac-address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4</td>
<td>7/BD-V/10/4/Up</td>
<td>0007.8508.4e50</td>
<td>000a.f331.1490</td>
</tr>
</tbody>
</table>
------------------------------------------
Total number of Active Session: 1

- show ethernet cfm pm session session-ID

Router# show ethernet cfm pm session 0
------------------------------------------
<table>
<thead>
<tr>
<th>EPM-ID</th>
<th>SLA-ID</th>
<th>Lvl/Type/ID/Cos/Dir</th>
<th>Src-Mac-address</th>
<th>Dst-Mac-address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>100</td>
<td>5/BD-V/2/4/Down</td>
<td>0000.0000.000b</td>
<td>0024.f951.85f1</td>
</tr>
</tbody>
</table>
------------------------------------------

- show ethernet cfm pm session detail session-ID

Router# show ethernet cfm pm session detail 0
Session ID: 0
Sla Session ID: 100
Level: 5
Service Type: BD-V
Service Id: 2
Direction: Down
Source Mac: 0000.0000.000b
Destination Mac: 0024.f951.85f1
Session Version: 0
Session Operation: On-demand
Session Status: Inactive
MPID: 1000
Tx active: no
Rx active: no
RP monitor Tx active: no
RP monitor Rx active: no
Timeout timer: stopped
Last clearing of counters: *03:55:07.670 UTC Mon Oct 1 2012

DMMs:
  Transmitted: 0
  Rcvd: 0

DMMs:
  Transmitted: 0
  Rcvd: 0

LMMs:
  Transmitted: 0
  Rcvd: 0

VMMs:
  Transmitted: 0
  Rcvd: 0

SLMs:
  Transmitted: 293
  Rcvd: 292

Test ID 1

- show ethernet cfm pm session inactive

Router# show ethernet cfm pm session inactive
Display of InActive Session

<table>
<thead>
<tr>
<th>EPM-ID</th>
<th>SLA-ID</th>
<th>Lvl/Type/ID/Cos/Dir</th>
<th>Src-Mac-address</th>
<th>Dst-Mac-address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>100</td>
<td>5/BD-V/2/4/Down</td>
<td>0000.0000.000b</td>
<td>0024.f951.85f1</td>
</tr>
</tbody>
</table>

Total number of Inactive Session: 1

- To display the IP SLA reaction configuration, use the show ip sla reaction-configuration command.

Router# show ip sla reaction-configuration
Entry number: 1
Reaction Configuration not configured

Entry number: 2
Index: 1
Reaction: loss-ratioSD
Threshold Type: Immediate
Rising: 50
Falling: 50
Action Type: None

Index: 2
Reaction: loss-ratioDS
Threshold Type: Immediate
Rising: 50
Falling: 50
Action Type: None

Index: 3
Reaction: unavailableSD
Threshold Type: Immediate
Rising: 50
Falling: 50
Action Type: None

Index: 4
Reaction: unavailableDS
Threshold Type: Immediate
Rising: 50
Falling: 50
Action Type: None

Troubleshooting

These troubleshooting scenarios apply to the Y.1731 performance monitoring configurations:

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When the IP SLA sessions do not come up.</td>
<td>Use these debug commands:</td>
</tr>
<tr>
<td></td>
<td>• debug ethernet cfm pm events [session &lt;session id&gt;]</td>
</tr>
<tr>
<td></td>
<td>• debug ethernet cfm pm error [session &lt;session id&gt;]</td>
</tr>
<tr>
<td></td>
<td>• debug ethernet cfm pm diagnostic</td>
</tr>
<tr>
<td></td>
<td>• debug ethernet cfm pm ipc [session &lt;session id&gt;]</td>
</tr>
<tr>
<td></td>
<td>• debug ethernet cfm pm packet [session &lt;session id&gt;]</td>
</tr>
<tr>
<td></td>
<td>• debug ethernet cfm pm monitor [session &lt;session id&gt;]</td>
</tr>
<tr>
<td></td>
<td>• debug platform npc epmpal all</td>
</tr>
<tr>
<td></td>
<td>• debug platform npc epmpal ecfm-events</td>
</tr>
<tr>
<td></td>
<td>• debug platform npc epmpal ecfm-info</td>
</tr>
<tr>
<td></td>
<td>• debug platform npc epmpal epm-trace</td>
</tr>
<tr>
<td></td>
<td>• debug platform npc epmpal errors</td>
</tr>
<tr>
<td></td>
<td>• debug platform npc epmpal events</td>
</tr>
<tr>
<td></td>
<td>• debug platform npc epmpal info</td>
</tr>
<tr>
<td></td>
<td>• debug platform npc epmpal packet</td>
</tr>
<tr>
<td></td>
<td>• debug platform npc epmpal statistics</td>
</tr>
</tbody>
</table>
IP and PPPoE Session Support

Intelligent Services Gateway (ISG) is a Cisco IOS software feature provides a structured framework for the edge devices to deliver flexible and scalable services to subscribers. ISG supports IP sessions for subscribers who connect to ISG from routed or Layer 2 access networks. From Cisco IOS Release 12.2(33)SRE onwards, the ISG: Subscriber Aware Ethernet feature provides Intelligent Services Gateway (ISG) functionality in distributed IP and PPPoE sessions on Cisco 7600 series routers that have Ethernet Services Plus (ES+) access-facing line cards.

IP sessions, representing a single IP address, collates the traffic received from a single IP source address, and classifies, identifies and provides services to subscribers. If the IP address is not unique, VRF or interface is used as unique identifiers. IP addresses can overlap only across VRF, and if two interfaces have the same VRF, they cannot have overlapping IP addresses. However, overlapping IP addresses are also supported for MAC based identification.

**Note**

Effective with Cisco IOS Release 15.2(4)S, the Broadband (IP and PPPoE sessions) support is deprecated in Cisco 7600 routers.

IP sessions are hosted for the following connected subscriber devices:

- Devices that are one hop far from SG are L2-connected sessions.
- Devices that are multiple hops from the system where Service Gateway (SG) is not at the extreme L3 edge are routed sessions.

This feature is supported on the following interfaces in a ES+ line card:

- Access interfaces
- Non-access interfaces (limited to 500 subinterfaces)

This feature supports the following sessions in a ES+ line card:

- IP sessions (routed and L2-connected)
- DHCP integration with IP sessions
- Static IP subnet sessions
- Source IP address and MAC address sessions (IP sessions)
- PPPoE supported in the PPP Termination and Aggregation (PTA) mode
- PPPoEoVLAN supported in the PTA mode
- PPPoEoQinQ supported in the PTA mode
- PPPoEoDot1Q supported in the PTA mode

**IP Address Assignment**

- DHCP Based IP address assignment: If DHCP is being used to assign IP addresses, and the IP address that is assigned by DHCP is correct for the service domain, ISG does not have to be involved in the assignment of an IP address for the subscriber. If the IP address that is assigned by DHCP is not correct for the service domain, or if the domain changes because of a VRF transfer, ISG can be configured to influence the DHCP IP address assignment.
- Static IP address assignment: If the static IP address for a subscriber is configured correctly for the service domain, ISG is not involved in the assignment of an IP address for the subscriber.
• IP subnet: For IP subnet sessions, the IP subnet is specified in the user profile.

IP interface: ISG is not involved in the assignment of subscriber IP addresses.

**IP Subnet (IP Range) Sessions**

A client subnet identifies an IP Subnet session and applies uniform edge processing to packets associated with a particular IP subnet. IP Subnet sessions are hosted for clients directly connected or over multiple hops. The following functionalities are not supported on IP Subnet Sessions, but are supported on IP Sessions:

- DHCP session initiation not supported
- No Source MAC address session support
- No Dynamic VPN selection support

**IP Interface Sessions**

In an IP Interface session, all the traffic received on a particular physical or logical interface is collated. However, dynamic VRF transfer is not supported in an IP interface session and, VRF transfer can only be used with static VRF configuration. Irrespective of the subscriber logged in, a session is created by default.

**PPPoE and IPoE Session Support on Port Channel (1:1 Redundancy)**

The 1:1 redundancy on a port channel coupled with Link Aggregation Control Protocol (LACP) dynamically handles the member links in a port channel bundle. A port channel has two members, of which one member is active and the other is in standby or redundant mode. The member ports can be across line cards, but must originate from Ethernet Services Plus (ES+) line card. At any given point of time, one link is on the physical mode.

The following sessions support 1:1 redundancy in a ES+ line card:

- IP Subnet sessions
- IP Interface sessions
- PPPoEoX sessions.

**Note**

Port channel sub-interfaces of type *access* provide M:N LAG support if the Intelligent Services Gateway (ISG) is not configured. In case the ISG is configured, only the 1:1 active–standby configuration is supported for *access* type sub-interfaces.

**PPPoE and IPoE Session Support on QinQ Subinterfaces with IEEE 802.1AH Customer Ethertype**

This feature enables you to implement PPPoE and IPoE session (ISG functions) on QinQ subinterfaces that are configured with custom ethertype. The custom ethertype implemented on the main interface is inherited by all the subinterfaces. To implement this feature, use `dot1q tunnel ethertype` command on main interface for the respective QinQ subinterfaces.
If the outer VLAN tag on a PPPoE or IPoE session packet matches the custom ethertype VLAN settings on the QinQ subinterface, the packets are accepted otherwise the packets are dropped. You can set the outer VLAN tag to the following values:

- 0x9100
- 0x9200
- 0x8100
- 0x88a8

The PPPoE or IPoE session does not come up if there is ethertype mismatch between ISG and the client. For example, if the outer VLAN tag on a packet is set to 0x9100 and the interface is configured using custom ethertype to accept only packets with 0x88a8 VLAN tag, the packet will be dropped in the QinQ subinterface.

You can configure QinQ on both the access and non-access sub-interfaces. The following code shows how to define an interface with access sub-interface, create a VLAN QinQ subinterface, and enable PPPoE session:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# dot1q tunneling ethertype 0x9100
Router(config-if)# interface gigabitethernet 1/0/0.100 access
Router(config-subif)# encapsulation dot1q 100 second-dot1q 200
Router(config-subif)# ip subscriber interface
```

### Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines when you configure an IP or a PPPoE sessions on an ES+ linecard:

- IP Sessions are not supported on ambiguous VLANs.
- Radius proxy is not supported for the IP Sessions.
- IP and MAC address spoof Prevention is not supported on subinterfaces on a ES+ linecard unlike on a SIP400 line card.
- IP sessions are supported on Link Aggregation (Ether-Channel) interfaces. LAG etherchannel interfaces are supported for links on the same and across line cards.
- PPPoE sessions are supported on ambiguous VLAN interfaces and VLAN ranges.
- There are no drop counters to identify the number of packets dropped due to custom ethertype mismatch.
- VLANs, Source MAC Address, and Ports are matched against session ids to extend security for PPPoE sessions.
- ES+ low queue cards do not support ISG (IP session and PPPoE session). From Cisco IOS Release 12.2(33)SRE8 onwards, Intelligent Services Gateway (ISG) will be disabled for ES+ Low Queue cards.

Follow these restrictions and usage guidelines when you configure 1:1 redundancy on a ES+ linecard:

- Subscriber redundancy is available only on a 1:1 access standby model.
- Supports access interfaces in port channels to scale the number of port channel subinterfaces to greater than 4k.
• Link Aggregation Control Protocol (LACP) allows dynamic handling of member links in a GEC bundle.
• Supports a maximum of 64 GEC bundles with 8 links.
• Member links in a single GEC bundle reside across NPs or the linecard.
• LAG is supported with members across linecards.
• Supports LAG across linecards and membership of the LAG does not change after new sessions are initiated.
• Feature supports 32000 access sub-interfaces.
• Supports per session load balancing across member links where all the traffic for a session is relayed over a single port.
• To reduce the downtime during member link addition or deletion, QOS queues are allocated for all member links belonging to the port channel. Though the ingress and egress traffic could be on different member links, the peer relays all the traffic for a session through a single member link.
• LAG supports sessions on non access subinterfaces to support coexistence of multicast streams.

**Verification**

This section lists the commands to display configuration information.

• Use the following commands to configure the PPPoE:

```
Router-DJ4-dfc9#sh debug
CWAN iEdge LC:
  CWAN iEdge LC session event debug debugging is on
X40G XLIF Client:
  XLIF NP events debugging is on

Router-DJ4-dfc9# sh log
Syslog logging: enabled (0 messages dropped, 4 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.
No Inactive Message Discriminator.

Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging: level debugging, 308 messages logged, xml disabled, filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

Log Buffer (1000000 bytes):

  seghandle 2CD93474 uid 40 if_number 80
Nov 19 16:08:48.247 IST: DFC9:  type 1 2 0opaque handle = 0x186DAB48
Nov 19 16:08:48.247 IST: DFC9: cwan_iedge_session_pending_timer started
Nov 19 16:08:48.247 IST: DFC9: no dbus_vlan session pending on int 105
  vlan 1020 through update for Virtual-Access2.1
Nov 19 16:08:50.247 IST: DFC9: cwan_iedge_common_session_notify: cfg_type 2 va_if_num
  105 phy_if_num 80 uid 0action 0
```
Nov 19 16:08:50.247 IST: DFC9: cwan_iedge_get_session_config: sess_type 2 if_num 105
pid 0
Nov 19 16:08:50.247 IST: DFC9: cwan_iedge_get_pppoe_config: if_num 80 va_if_num 105
vlan 1020 sess-id 40 cond_debug off
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_create Cfn[965F2BC] Creating Xlif:
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_create_internal successfully created
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_eg_xlif_update_port Cfn[92D1658] Xlif Update
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_tag_rewrite Cfn[965F334] Tag(i-0,
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_dbus_vlan Cfn[965F36C] Updateing
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_stats_id Cfn[965D780] Updatng
Stats Id 599056 Dir[0]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352] ef[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_fwd_feat_enable Cfn[965F3BC] Xlif Fwd
Feat 0x1 Enable 1 : GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352] ef[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_enable Cfn[965F5C0] Xlif Enable 1:
feature Dir[0]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352] ef[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_feature_info Cfn[965F700] Xlif update

Router-DJ4#sh debug
PPP:
  PPP protocol negotiation debugging is on
  PPPoE:
  PPPoE protocol events debugging is on
  PPPoE control packets debugging is on

Router-DJ4#sh log
Syslog logging: enabled (3340 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging: level debugging, 5280 messages logged, xml disabled, filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

Trap logging: level informational, 203 message lines logged

Log Buffer (1000000 bytes):
Nov 19 16:08:48.231 IST: PPPoE 0: I PADI  R:bb00.1912.0001 L:ffff.ffff.ffff 2 Gi9/5.1 contiguous pak, size 60
FF FF FF FF FF BB 00 19 12 00 01 81 00 00 02
88 63 11 09 00 00 00 04 01 01 00 00 00 0A 03 06
B6 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00
00 00 00 00 00 00 06 F8 00 00 9C 88
Nov 19 16:08:48.231 IST: Service tag: NULL Tag
Nov 19 16:08:48.231 IST: PPPoE 0: O PADO, R:a110.0050.0006 L:bb00.1912.0001 1019 Gi9/5.1
Nov 19 16:08:48.231 IST: Service tag: NULL Tag
contiguous pak, size 100
06 02 00 10 03 FB 28 00 03 80 00 00 44 00 00 00
00 00 00 00 00 00 00 00 00 00 00 02 04 00 00
BB 00 19 12 00 01 A1 10 00 50 00 68 81 00 00 02
88 63 11 07 00 00 00 24 01 01 00 00 01 02 00 08
82 69 61 7A 2D 44 4A ...
IP and PPPoE Session Support

Chapter 4  Configuring Layer 1 and Layer 2 Features

Nov 19 16:08:48.235 IST: ppp40 LCP: I CONFACK [ACKsent] id 1 len 18
Nov 19 16:08:48.235 IST: ppp40 LCP: MRU 1492 (0x010405D4)
Nov 19 16:08:48.235 IST: ppp40 LCP: AuthProto CHAP (0x0305C22305)
Nov 19 16:08:48.235 IST: ppp40 LCP: MagicNumber 0x0F501712 (0x05060F501712)
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is AUTHENTICATING, by this end
Nov 19 16:08:48.243 IST: ppp40 CHAP: 0 CHALLENGE id 1 len 29 from "Router-DJ4"
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is FORWARDING, Attempting Forward
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is AUTHENTICATING, Unauthenticated User
Nov 19 16:08:48.243 IST: ppp40 IPCP: Authorizing CP
Nov 19 16:08:48.243 IST: ppp40 IPCP: CP stalled on event[Authorize CP]
Nov 19 16:08:48.243 IST: ppp40 IPCP: CP uninstalled
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is FORWARDING, Attempting Forward
Nov 19 16:08:48.243 IST: [40]PPPoE 40: State LCP_NEGOTIATION Event SSS CONNECT LOCAL
Nov 19 16:08:48.247 IST: [40]PPPoE 40: Segment (SSS class): UPDATED
Nov 19 16:08:48.247 IST: [40]PPPoE 40: Segment (SSS class): BOUND
Nov 19 16:08:48.247 IST: [40]PPPoE 40: data path set to Virtual Access
Nov 19 16:08:48.247 IST: [40]PPPoE 40: State LCP_NEGOTIATION Event SSM UPDATED
Nov 19 16:08:48.247 IST: Vi2.1 PPP: Phase is AUTHENTICATING, Authenticated User
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: O CONFREQ [Starting] id 1 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: I CONFREQ [REQsent] id 0 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Address 0.0.0.0 (0x030600000000)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP AUTHOR: Start. Her address 0.0.0.0, we want 0.0.0.0
Nov 19 16:08:48.247 IST: Vi2.1 IPCP AUTHOR: Done. Her address 0.0.0.0, we want 0.0.0.0
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Pool returned 182.0.0.1
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: O CONFNAK [REQsent] id 0 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: I CONFACK [REQsent] id 1 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Address 100.0.0.1 (0x030664000001)
Nov 19 16:08:48.247 IST: [40]PPPoE 40: State PTA_BINDING Event STATIC BIND RESPONSE
Chapter 4      Configuring Layer 1 and Layer 2 Features
IP and PPPoE Session Support

Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Address 100.0.0.1 (0x030664000001)
Nov 19 16:08:48.275 IST: Vi2.1 IPCP: State is Open (Indicates that the PPPoE session is up)
Nov 19 16:08:48.275 IST: Vi2.1 Added to neighbor route AVL tree: topoid 0, address 182.0.0.1
Nov 19 16:08:48.275 IST: Vi2.1 IPCP: Install route to 182.0.0.1

Router-DJ4#

interface GigabitEthernet9/17.1
    encapsulation dot1Q 2000
    ip address 180.0.0.1 255.255.255.0

interface GigabitEthernet9/5.1
    encapsulation dot1Q 2
    ip address 192.0.0.1 255.255.255.0
    pppoe enable group dj4_bba_group1

aaa new-model
aaa authentication login default group radius local
aaa authentication ppp default local
aaa authorization network default local
aaa authorization subscriber-service default group radius
aaa session-id common

bba-group pppoe dj4_bba_group1
virtual-template 1
    sessions per-vc limit 16000
    sessions per-mac limit 16000
    sessions per-vlan limit 8000

interface Loopback1
    ip address 100.0.0.1 255.255.255.255

interface Virtual-Template1
    ip unnumbered Loopback1
    no logging event link-status
    peer default ip address pool PPPPool_1
    no snmp trap link-status
    keepalive 300
    ppp authentication chap

- Use the following commands to verify the PPPoE session:

Router-DJ4#sh pppoe summary
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)

<table>
<thead>
<tr>
<th></th>
<th>TOTAL</th>
<th>PTA</th>
<th>FWDED</th>
<th>TRANS</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet9/5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Router-DJ4#sh pppoe ses</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Router-DJ4#sh pppoe session
1 session  in LOCALLY_TERMINATED (PTA) State
1 session  total

Uniq ID  PPPoE  RemMAC  Port  VT  VA  State
SID  LocMAC

CISCO 7600 SERIES ETHERNET SERVICES PLUS (ES+) AND ETHERNET SERVICES PLUS T (ES+T) LINE CARD CONFIGURATION GUIDE
OL-16147-29
Chapter 4      Configuring Layer 1 and Layer 2 Features

IP and PPPoE Session Support

42 42 bb00.1912.0001  Gi9/5.1  1 Vi2.1  PTA
000c.31c9.7000  VLAN: 2
Router-DJ4#sh sss session uid 42 detailed
Unique Session ID: 42
Identifier: PPP_USER
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:19:04, Last Changed: 00:19:04
Interface: Virtual-Access2.1

Policy information:
  Context 137426FC: Handle 2400002A
  AAA_id 00000038: Flow_handle 0
  Authentication status: authen
  Downloaded User profile, excluding services:
    Framed-Protocol 1 [PPP]
    username "PPP_USER"
  Downloaded User profile, including services:
    Framed-Protocol 1 [PPP]
    username "PPP_USER"
Config history for session (recent to oldest):
  Access-type: PPP Client: SM
  Policy event: Process Config Connecting
  Profile name: apply-config-only, 2 references
    Framed-Protocol 1 [PPP]
    username "PPP_USER"
Rules, actions and conditions executed:
  subscriber rule-map PPPoE-SUB
  condition always event session-start
  1 service local

Configuration sources associated with this session:
  Interface: Virtual-Templat1, Active Time = 00:19:04

Router-DJ4# sh pppoe session packets
Total PPPoE sessions 1

<table>
<thead>
<tr>
<th>SID</th>
<th>Pkts-In</th>
<th>Pkts-Out</th>
<th>Bytes-In</th>
<th>Bytes-Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>12</td>
<td>13</td>
<td>184</td>
<td>190</td>
</tr>
</tbody>
</table>

Router-DJ4# sh cef int gig 9/5.1
GigabitEthernet9/5.1 is up (if_number 80)
  Corresponding hwidb fast_if_number 80
  Corresponding hwidb firstsw->if_number 25
  Internet address is 192.0.0.1/24
  ICMP redirects are always sent
  IP unicast RPF check is disabled
  Output features: MFIB Adjacency, HW Shortcut Installation
  IP policy routing is disabled
  BGP based policy accounting on input is disabled
  BGP based policy accounting on output is disabled
  Hardware idb is GigabitEthernet9/5
  Fast switching type 28, interface type 146
  IP CEF switching enabled
  IP CEF switching turbo vector
  IP Null turbo vector
  IP prefix lookup IPv4 mtrie generic
  Input fast flags 0x40000000, Output fast flags 0x0
  ifindex 24(24)
  Slot 9/0 (9) Slot unit 5 VC -1
  IP MTU 1500
Use the following commands to configure IP session:

```bash
aaa new-model
!
aaa session-id common
!
interface GigabitEthernet2/9
  no ip address
  load-interval 30
!
interface GigabitEthernet2/9.1 access
  encapsulation dot1Q 2 second-dot1q 2
  ip address 182.0.0.1 255.255.255.0
  ip subscriber routed
  initiator unclassified ip-address
!
interface GigabitEthernet2/10
  no ip address
  load-interval 30
!
interface GigabitEthernet2/10.1
  encapsulation dot1Q 2000 second-dot1q 2001
  ip address 180.0.0.1 255.255.255.0
!
  no ip http server
  no ip http secure-server
!
  arp 182.0.0.2 aa00.0000.0001 ARPA
  arp 180.0.0.2 0000.0000.0001 ARPA
```

Use the following commands to debug IP session:

```bash
ISG_NMB#sh deb
CWAN iEdge RP:
  CWAN iEdge RP debug debugging is on

IP Subscriber:
  all IP subscriber debugs debugging is on
ISG_NMB#
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Insert new entry for mac 0000.1500.0001
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Processing new in-band session request
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Delete mac entry 0000.1500.0001
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] In-band session request event for session
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Added upstream entry into the classifier
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] VRF = DFL, IP = 21.0.0.1, MASK = 255.255.255.255
Nov 19 16:02:46.087 IST: IPSUB: Try to create a new session
Nov 19 16:02:46.087 IST: IPSUB: IPSUB: Check IP DHCP session recovery: 21.0.0.1
Gi2/9.1 mac aa00.0000.0001
Nov 19 16:02:46.087 IST: IPSUB: IPSUB: No DHCP binding found
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] IPSUB: Proceed to create the IP inband session
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] Request to create a new session
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] Session start event for session
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] Event session start, state changed from idle to requesting
Nov 19 16:02:46.087 IST: IPSUB: HA[uid:32]: Session init-notification on Active
Nov 19 16:02:46.087 IST: IPSUB: HA[uid:32]: Allocated SHDB handle (0xF1000020)
Nov 19 16:02:46.087 IST: IPSUB: HA[uid:32]: Successfully initialized for HA
```
IP and PPPoE Session Support

Chapter 4  Configuring Layer 1 and Layer 2 Features

Use the following commands to verify IP session:

```
ISG_NMB#sh ip sub
Displaying subscribers in the default service vrf:

<table>
<thead>
<tr>
<th>Type</th>
<th>Subscriber Identifier</th>
<th>Display UID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>routed</td>
<td>21.0.0.1/32</td>
<td>[32]</td>
<td>up</td>
</tr>
</tbody>
</table>

ISG_NMB#
```

ISG_NMB#sh sss sess
Current Subscriber Information: Total sessions 1
IP and PPPoE Session Support

Chapter 4 Configuring Layer 1 and Layer 2 Features

<table>
<thead>
<tr>
<th>Uniq ID</th>
<th>Interface</th>
<th>State</th>
<th>Service</th>
<th>Identifier</th>
<th>Up-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>IP</td>
<td>unauthen</td>
<td>Local Term</td>
<td>21.0.0.1</td>
<td>00:02:40</td>
</tr>
</tbody>
</table>

Uniq ID Interface State Service Identifier Up-time
32  IP  unauthen  Local Term 21.0.0.1 00:02:40

ISG_NMB#sh sss sess uid 32
Unique Session ID: 32
Identifier: 21.0.0.1
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:02:46, Last Changed: 00:02:46

Policy information:
Authentication status: unauthen

Configuration sources associated with this session:
Interface: GigabitEthernet2/9.1, Active Time = 00:02:46

ISG_NMB#sh sss sess uid 32 de
ISG_NMB#sh sss sess uid 32 detailed
Unique Session ID: 32
Identifier: 21.0.0.1
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:02:49, Last Changed: 00:02:49

Policy information:
Context 133B22FC: Handle DF000020
AAA_id 00000030: Flow_handle 0
Authentication status: unauthen

Configuration sources associated with this session:
Interface: GigabitEthernet2/9.1, Active Time = 00:02:49

Following details is for a L2-connected DHCP session on Dot1Q interface:

• Use the following commands to configure L2-connected DHCP session:

  aaa new-model
  
  aaa session-id common
  
  clock timezone IST 5
  ip source-route
  
  ip dhcp excluded-address 182.0.0.11 182.0.0.15
  no ip dhcp ping packets
  
  ip dhcp pool pool_global1
      network 182.0.0.0 255.255.255.240
      lease 0 0 3
     update arp
  
  interface Loopback10
      ip address 182.0.0.11 255.255.255.255


IP and PPPoE Session Support

Chapter 4 Configuring Layer 1 and Layer 2 Features

IP and PPPoE Session Support

! interface GigabitEthernet2/9
    no ip address
    load-interval 30
!
interface GigabitEthernet2/9.1 access
    encapsulation dot1Q 2
    ip unnumbered Loopback10
    ip subscriber 12-connected
    initiator dhcp class-aware
!
interface GigabitEthernet2/10
    no ip address
    load-interval 30
!
interface GigabitEthernet2/10.1
    encapsulation dot1Q 2000
    ip address 180.0.0.1 255.255.255.0
!
!
no ip http server
no ip http secure-server
ip route 7.0.0.0 255.0.0.0 7.38.0.1
ip route 202.153.0.0 255.255.0.0 7.38.0.1
!
!
• Use the following commands to debug L2-connected DHCP session:

    ISG_NMB#sh deb
    DHCP server packet debugging is on.
    DHCP server event debugging is on.

    IP Subscriber:
    IP subscriber events debugging is on
    IP subscriber errors debugging is on
    IP subscriber packets debugging is on

    ISG_NMB#
    results = 0x40
    IP routing
    tableid 0.
    Nov 19 15:40:33.595 IST: DHCPD: tableid for 182.0.0.11 on GigabitEthernet2/9.1 is 0
    Nov 19 15:40:33.595 IST: DHCPD: Sending notification of DISCOVER:
    Nov 19 15:40:33.595 IST: DHCPD: htype 1 chaddr aa00.1314.0001
    Nov 19 15:40:33.595 IST: DHCPD: remote id 020a0000b600000b21010002
    Nov 19 15:40:33.595 IST: DHCPD: class id 49786961
    Nov 19 15:40:33.595 IST: IPSUB: Create session keys from SSS key list
    Nov 19 15:40:33.595 IST: IPSUB: Mac_addr = aa00.1314.0001, Recvd Macaddr = aa00.1314.0001
    Nov 19 15:40:33.599 IST: IPSUB: Session input interface(0x13348754) =
    GigabitEthernet2/9.1
    Nov 19 15:40:33.599 IST: IPSUB: SHDB Handle = 5A00000B
    Nov 19 15:40:33.599 IST: IPSUB: Remote_id = 020a0000b600000b21010002
    Nov 19 15:40:33.599 IST: IPSUB: Vendor_Class_id = Ixia
    Nov 19 15:40:33.599 IST: DHCPD: DHCPDISCOVER received from client 01aa.0013.1400.01 on
Nov 19 15:40:33.599 IST: DHCPD: Sending notification of DISCOVER:
Nov 19 15:40:33.599 IST: DHCPD: htype 1 chaddr aa00.1314.0001
Nov 19 15:40:33.599 IST: DHCPD: remote id 020a0000b600000b21010002
Nov 19 15:40:33.599 IST: DHCPD: class id 49786961
Nov 19 15:40:33.599 IST: DHCPD: Saving workspace (ID=0x8900000B)
Nov 19 15:40:33.599 IST: DHCPD: New packet workspace 0x1333D0D8 (ID=0x2700000C)
Nov 19 15:40:33.599 IST: IPSUB: Try to create a new session
Nov 19 15:40:33.599 IST: IPSUB: [uid:0] Request to create a new session
Nov 19 15:40:33.599 IST: IPSUB: [uid:0] Session start event for session
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Added session aa00.1314.0001 to L2 session table
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Added session to session table with access session keys
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] IP session(0xC500000B) to be associated to Gi2/9.1
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Inserted IP session(0xC500000B) to sessions-per-interface db with interface Gi2/9.1
Nov 19 15:40:33.599 IST: DHCPD: Callback for workspace (ID=0x8900000B)
Nov 19 15:40:33.599 IST: DHCPD: No authentication required. Continue
Nov 19 15:40:33.599 IST: DHCPD: Reprocessing saved workspace (ID=0x8900000B)
Nov 19 15:40:33.599 IST: DHCPD: tableid for 182.0.0.11 on GigabitEthernet2/9.1 is 0
Nov 19 15:40:33.599 IST: DHCPD: Adding binding to radix tree (182.0.0.11) is 0
Nov 19 15:40:33.599 IST: DHCPD: Adding binding to hash tree
Nov 19 15:40:33.599 IST: DHCPD: assigned IP address 182.0.0.1 to client 01aa.0013.1400.01. (13 1)
Nov 19 15:40:33.599 IST: DHCPD: DHCPofffer notify setup address 182.0.0.1 mask 255.255.255.240
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] IP session context 0x133D28C8 available to authorize
Nov 19 15:40:33.599 IST: IPSUB-VRFSSET: [uid:11] Allocated sg vrfsset info 0x13488EE0
Nov 19 15:40:33.599 IST: IPSUB-VRFSSET: [uid:11] Freeing the sg vrfsset info 0x13488EE0
Nov 15:40:33.599 IST: IPSUB: [uid:11] Got IP address- IP:-182.0.0.1
Nov 15:40:33.599 IST: IPSUB: [uid:11] Set IP address- IP:-182.0.0.1
Nov 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Checking whether routes to be inserted/removed
0x1348DD04
Nov 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Installed ARP entry [DFL]: 182.0.0.1
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Both IP addresses and VRF are same, no need to add route
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Found that seg to be updated with new session keys
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Key list to be created to update SM
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Created key list to update SM
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Found address change to be notified
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Added session 182.0.0.1 to L3 session table
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Added session to session table with service session keys
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Received Message = update SIP config
Nov 19 15:40:33.603 IST: IPSUB-ROUTE: [uid:11] Checking whether routes to be inserted/removed
Nov 19 15:40:33.603 IST: IPSUB-ROUTE: [uid:11] Ctx present, No config change, Nothing to be done
Nov 19 15:40:33.603 IST: IPSUB-ROUTE: [uid:11] Both IP addresses and VRF are same, no need to add route
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Created key list to update SM
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Notifying about address change: 182.0.0.1
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Key list to be created to update SM
Nov 19 15:40:33.603 IST: DHCPD: Callback: switching path now setup for client 01aa.0013.1400.01
Nov 19 15:40:33.603 IST: DHCPD: Reprocessing saved workspace (ID=0x8900000B)
Nov 19 15:40:33.603 IST: DHCPD: Sending notification of DISCOVER:
Nov 19 15:40:33.603 IST: DHCPD: htype 1 chaddr aa00.1314.0001
Nov 19 15:40:33.603 IST: DHCPD: remote id 020a0000b600000b21010002
Nov 19 15:40:33.603 IST: DHCPD: class id 49786961
Nov 19 15:40:33.603 IST: DHCPD: DHCPDISCOVER received from client 01aa.0013.1400.01 on interface GigabitEthernet2/9.1.
Nov 19 15:40:33.603 IST: DHCPD: Found previous server binding
Nov 19 15:40:33.603 IST: DHCPD: Sending DHCPOFFER to client 01aa.0013.1400.01 (182.0.0.1).
Nov 19 15:40:33.603 IST: DHCPD: ARP entry exists (182.0.0.1, aa00.1314.0001).
Nov 19 15:40:33.603 IST: DHCPD: unicasting BOOTREPLY to client aa00.1314.0001 (182.0.0.1).
Nov 19 15:40:33.603 IST: DHCPD: removing ARP entry (182.0.0.1 vrf default).
Nov 19 15:40:33.603 IST: DHCPD: Freeing saved workspace (ID=0x8900000B)
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:0] Setup event for session (session hdl 0)
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:0] Insert new entry for mac aa00.1314.0001
IP and PPPoE Session Support

Use the following commands to verify L2-connected DHCP session:

```
ISG_NMB#sh ip dhcp binding
Bindings from all pools not associated with VRF:
  IP address  Client-ID/  Lease expiration  Type  Hardware address/  User name
  182.0.0.1   01aa.0013.1400.01 Nov 19 2009 03:45 PM Automatic

ISG_NMB#sh sss session
Current Subscriber Information: Total sessions 1

Uniq ID Interface  State  Service  Identifier  Up-time
11 IP  unauthen  Local Term  aa00.1314.0001  00:00:58

ISG_NMB#sh sss session uid 11
Unique Session ID: 11
Identifier: aa00.1314.0001
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:01:04, Last Changed: 00:01:04

Policy information:
  Authentication status: unauthen

Configuration sources associated with this session:
  Interface: GigabitEthernet2/9.1, Active Time = 00:01:04
```

```
IP and PPPoE Session Support

Troubleshooting

The following troubleshooting scenarios are applicable to the broadband technology area:

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When a subinterface is configured for IP sessions and the ISG policy map has been configured to perform some actions, the IP session does not come up.</td>
<td>Use the <code>show</code> and <code>debug</code> commands to confirm if the ISG policymap configuration is correct.</td>
</tr>
<tr>
<td>A subinterface is configured for IP sessions – initiator DHCP. ISG policymap applied on subinterface is for Transparent Autologon (TAL). The user profile downloaded has the classname pointing to DHCP pool and the session is not initiated.</td>
<td>Check if the DHCP pool referred by the downloaded classname in the user profile is not in the same subnet as the subinterface loopback interface. If yes, correct the subnet value to re-initiate the session.</td>
</tr>
<tr>
<td>10 ports on two v2 SPAs are connected to traffic generator on access side. One 10 Gigabyte port (6704 card) is connected to the TGEN on the core side. Traffic for triple play (video, voice and data) is being sent on egress. The line card is heavily oversubscribed – voice: 400 Mbps, Video: 3 Gbps, Data: 5 Gbps. Despite video and voice being classified as priority, video traffic drops while data traffic is stable.</td>
<td>Mark the preceding values in video class of service to 6 or 7.</td>
</tr>
<tr>
<td>An IP session is enabled on a subinterface where the DHCP initiator is configured in a routed mode. Traffic in the upstream and downstream directions is enabled. The traffic generator indicates that traffic is not received and is dropped by router and the traffic generator on the access side does not respond to the Address Resolution Protocol (ARP).</td>
<td>Check the adjacencies and use the ARP to locate the problem.</td>
</tr>
<tr>
<td>A subinterface is configured for an IP session and an ISG policymap configured with police, default-drop actions is applied. Once the session is enabled, it is automatically disabled within a few seconds.</td>
<td>The ISG policymap actions force the session to authenticate and disconnect after 5 seconds if authentication fails as radius server does not authenticate the session. Use the <code>test aaa</code> command to check if the radius authenticates the sessions.</td>
</tr>
</tbody>
</table>
### Chapter 4  Configuring Layer 1 and Layer 2 Features

#### IP and PPPoE Session Support

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP session is disabled before the specific time</td>
<td>Use the <code>show ip subscriber</code> command with the <code>dangling</code> keyword to display dangling sessions. The <code>seconds</code> argument allows you to specify how long the session has to remain unestablished before it is considered dangling.</td>
</tr>
<tr>
<td>Issues with trace subscriber sessions, errors, events, session state changes, and session packets in the ISG IP subscriber sessions.</td>
<td>To enable ISG IP subscriber session debugging, use the <code>debug ip subscriber</code> command in privileged EXEC mode.</td>
</tr>
<tr>
<td>If a policy-map is applied on the sub-interface and a QoS session is enabled, the session is initiated, but QoS is not installed on it.</td>
<td>Apply the QoS policy-map either on the session or on the sub-interface, but not on both at the same time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you set classification and marking on an ISG subscriber session, an error is displayed when the session is initiated.</td>
<td>Check if you have configured the CoS inner and ACL combination. If yes, unconfigure and reconfigure them separately.</td>
</tr>
</tbody>
</table>
| Class SSS: (QoS) - install error is displayed.                          | • The error could be a problem with the QoS installation on the session due to:  
  • Invalid QoS policymap  
  • QoS session is already applied on the subinterface.  
  If both these checks are negative, contact TAC. |
| Multiple issues with Control Plane Policing installation and rate limiting. | Use the `show platform copp rate-limit <arp|dhcp|all>` exec-mode command to display the list of interfaces on which a rate limiter is active for the given protocol(s) (either for a single protocol, or for all protocols) along with the count of conformed or exceeded packets for the rate limiter. Remaining observation period is displayed on rate limiter enabled interfaces. |
| Packets are not limited by rates                                       | Ensure that the interface is enabled and check for these conditions:  
  • Check the class-map and ensure that it has the right protocol and keyword access.  
  • Check the policy-map and ensure that it has the right class-map.  
  • Check if the `conform-action` is set to `transmit` to avoid rate-limited packet drops.  
  • Ensure that the service-policy is applied on all the access subinterfaces.  
  • Use the `show platform copp rate-limit <protocol-name>` command to check if the policers are configured in the protocol and rate value is configured within the policy map. |
Per Subscriber Session Call Admission Control (CAC)

In broadband networks, ISG might receive a large number of incoming requests during peak hours. Each session that attempts to establish a connection on the ISG consumes a considerable amount of CPU and memory resources of the ISG. External resources, such as a remote authentication dial in user service (RADIUS) might not be able to handle all the requests that ISG generates. Accepting too many calls might make the router inefficient in its operation, overloading its own CPU, and also RADIUS. Per subscriber session CAC is a function that protects the router and external peripherals from getting overloaded by limiting the number of incoming calls based on CPU and session charges that a router can establish.

The route processor (RP) in the ISG checks CPU utilization and session charges to determine if a call should be accepted or rejected as follows:

- CPU utilization—The RP uses the 5-second average system variable that provides a cumulative average of the CPU usage percentage over a period of one minute to determine the average CPU usage percentage allowed on the system and compares that to the current CPU load. The CAC accepts the call only if the current CPU load is below the system variable limit, else rejects the call.
- Session charges—The RP compares the existing outstanding session charges to a user-configurable system variable. The CAC accepts the call and adds the session charges only if the session charges are below the system variable limit, else CAC rejects the call.

Restrictions and Guidelines

The restrictions and guidelines for per subscriber session CAC is given as follows:

- CAC is supported on PPPoE and IP sessions. For PPPoE sessions, both CPU and session charge based CAC is available. On IP sessions, only CPU based CAC is supported.
- DHCP sessions are not supported for CAC.

Implementing CAC

The CAC implementation impacts two queues - the First Sign of Life (FSOL) queue and the FSOL control queue. The default values for the FSOL queue and FSOL control queue are given in Table 4-44.

Whenever the CAC starts, the configured queue values for the actual FSOL and FSOL control queues are saved and the default values in Table 4-44 are installed on the line card. Whenever the CAC is stopped, the configured values (the values that are saved when the CAC is started) are restored. You can use the `hw-module slot slot_num rate-limit fsol_rate rate` command to configure the queue values. If you execute the command and configure the queue values while CAC is on, the new values overwrite the existing queue values that are saved and when the CAC is stopped, the new values are installed.

The CAC is implemented at the queue level even though the configuration accepts rate limit. The configuration changes are applied on a per network processor (NP) basis.

<table>
<thead>
<tr>
<th>Queue Name</th>
<th>Queue Depth</th>
<th>Shape Rate in bps</th>
<th>CAC Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual FSOL</td>
<td>100</td>
<td>40000</td>
<td>Off</td>
</tr>
<tr>
<td>FSOL control</td>
<td>900</td>
<td>360000</td>
<td>Off</td>
</tr>
</tbody>
</table>
Configuring Per Subscriber Session CAC

To configure per subscriber session CAC, perform these steps:

Summary Steps

1. enable
2. configure terminal
3. call admission new-model
4. call admission cpu-limit limit
   or
5. call admission limit charge
6. call admission type charge lifetime
7. end

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: enable Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: configure terminal Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 call admission new-model</td>
<td>Enables the new model of CAC.</td>
</tr>
<tr>
<td>Example: call admission new-model Router(config)# call admission new-model</td>
<td></td>
</tr>
</tbody>
</table>
### Per Subscriber Session Call Admission Control (CAC)

#### Configuration Example

The following example configures a charge of 10 per session and a call admission limit of 50, which allows calls at a rate of 5 calls per second:

```bash
Router# enable
Router# configure terminal
Router(config)# call admission new-model
Router(config)# call admission limit 50
Router(config)# call admission pppoe 10 1
Router# end
```

**Verifying and Monitoring Per Subscriber Session CAC**

To verify and monitor per subscriber session CAC, use either of these commands in privileged EXEC mode:

#### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td><code>call admission cpu-limit limit</code></td>
<td>Configures CAC based on CPU utilization.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# call admission cpu-limit 90</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Ensure that you do not set the CPU threshold value too low. The recommended value is between 80 to 90 percent.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>call admission limit charge</code></td>
<td>Configures CAC based on the session charge by specifying the maximum value of the total outstanding session charges to start CAC and reject calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# call admission limit 90</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>charge</code></td>
<td>The maximum value of the outstanding session charges. Valid values are from 0 to 100,000.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>call admission type charge lifetime</code></td>
<td>Specifies the call charge to add per session.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# call admission pppoe 10 1</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>type</code></td>
<td>Specifies the type of session charge profile.</td>
</tr>
<tr>
<td></td>
<td><code>charge</code></td>
<td>Specifies the per-session charge. Valid values are from 0 to 1000. The recommended value is 10.</td>
</tr>
<tr>
<td></td>
<td><code>lifetime</code></td>
<td>Specifies the session lifetime. Valid values are from 1 to 31. The recommended value is 1.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>end</code></td>
<td>Exits the global configuration mode.</td>
</tr>
</tbody>
</table>
Configuring Private Host on Pseudoport on CWAN Cards

The Private Hosts feature allows automatic insertion of router Switched Virtual Interface (SVI) MAC into the Private Hosts configuration. Private Hosts track the Layer 2 port that a server is connected to and limits undesired traffic through the MAC-layer ACLs. Hosts can carry multiple traffic types through the trunk port, remain isolated from each other, and still communicate to a common server. For more information on this feature and on Private Hosts, see Cisco 7600 Series Cisco IOS Software Configuration Guide, 15.0SR at http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/pacl.html

Configuring Unidirectional Link Detection (UDLD) on Ports with EVCs

UDLD (Unidirectional Link Detection) is a Layer 2 protocol that interacts with a Layer 1 protocol to determine the physical status of a link. At Layer 1, physical signaling and fault detection is auto-negotiated. UDLD detects the neighbor link, identifies, and disables the wrongly connected LAN ports. When you enable auto-negotiation and UDLD, Layer 1 and Layer 2 detections prevent physical and logical unidirectional connections, and malfunctioning of other protocols.

A unidirectional link occurs when the neighbor link receives the traffic transmitted by the local device, but the local device does not receive the transmitted traffic from its neighbor. If auto-negotiation is active, and one of the fiber strands in a pair is disconnected, the link is disabled. The logical link is undetermined, and UDLD does not take any action. At Layer 1, if both fibers are normal, UDLD at Layer 2 determines if the fibers are accurately connected, and traffic is relayed bidirectionally between the right neighbors. In this scenario, auto-negotiation operates in Layer 1, and the link status is unchecked.

The UDLD protocol monitors physical configuration of the cables, and detects unidirectional links of devices connected to LAN ports via Ethernet cables. When a unidirectional link is detected, UDLD disables the affected LAN port, and alerts the user.

The Cisco 7600 series router periodically transmits UDLD packets to neighboring devices on LAN ports with UDLD. If the packets are returned within a specific time frame, and there is no acknowledgement, the link is flagged as unidirectional, and the LAN port is disabled.

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines while configuring UDLD on ports with EVCs:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show call admission statistics</td>
<td>Displays statistical information about CAC operation and whether the new CAC model is enabled or not.</td>
</tr>
<tr>
<td>show platform isg fsol-queue-statistics</td>
<td>Displays the number of packets dropped in a line card for a specific queue. This command is available only on ES+ line cards.</td>
</tr>
</tbody>
</table>
Configuring Unidirectional Link Detection (UDLD) on Ports with EVCs

- You can configure UDLD only on a port.
- To identify and disable the unidirectional links, devices at both ends must support UDLD.
- Service bridge domain should be available on the router.
- Any of the supported EVC encapsulation can be configured.
- Cisco IOS Release 15.1(1)S supports EVC port-channels.

**Note**

If UDLD is enabled on an EVC port with service type **connect** or **xconnect** and encapsulation type **default** or **untagged**, the port is disabled.

For more information on UDLD, see the *Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SR* at the following URL:


### Configuring UDLD Aggressive Mode

As UDLD aggressive mode is disabled by default, you can configure UDLD aggressive mode in point-to-point links between network devices that support UDLD aggressive mode.

When UDLD aggressive mode is enabled:

- A port on a bidirectional link with UDLD neighbor relationship does not receive UDLD packets.
- UDLD tries to reestablish the connection with the neighbor.
- After eight failed retries, the port is disabled.

To prevent spanning tree loops, ensure that you set the non aggressive UDLD value interval to 15 seconds. This disables the unidirectional link before blocking the port transitions in the forwarding state (with default spanning tree parameters).

The benefits of enabling UDLD aggressive mode are:

- Port on one side of a link is disabled (both Tx and Rx).
- One side of a link is enabled even if the other side of the link fails.

In the above scenario, UDLD aggressive mode disables the port that prevents traffic from being discarded.

<table>
<thead>
<tr>
<th>If UDLD...</th>
<th>Then the...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detects a unidirectional link,</td>
<td>interface with its EVCs are disabled.</td>
</tr>
<tr>
<td>Is enabled on a port with an EVC bridge-domain,</td>
<td>selected EVC is not shut down, and prevents the</td>
</tr>
<tr>
<td>and encapsulation value set to default or</td>
<td>port from being disabled.</td>
</tr>
<tr>
<td>untagged,</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling UDLD on Ports With EVC Configured

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `{udld | no udld} enable aggressive`  
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2 <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3 `{udld</td>
<td>no udld} enable aggressive`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# udld enable aggressive</code></td>
<td></td>
</tr>
<tr>
<td>Step 4 <code>exit</code></td>
<td>Exits configuration mode.</td>
</tr>
</tbody>
</table>

**SUMMARY STEPS**

1. `interface type/ slot/ port`
2. `{udld port | no udld port } aggressive`
3. `show udld type/ slot/ port`
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>interface type/ slot/ port</code></td>
<td>Selects the LAN port to configure.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# gigethernet 1/0/0</code></td>
<td></td>
</tr>
<tr>
<td>Step 2 `{udld port</td>
<td>no udld port } aggressive`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# udld port aggressive</code></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# no udld port aggressive</code></td>
<td>Disables a UDLD on a non- fiber-optic LAN port.</td>
</tr>
</tbody>
</table>
### Configuring Unidirectional Link Detection (UDLD) on Ports with EVCs

#### Disabling Individual UDLD on Ports With EVC Configured

**SUMMARY STEPS**

1. `interface type/ slot/ port`
2. `{udld port | no udld port } disable`
3. `show udld type/ slot/ port`
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td><code>show udld type/ slot/ port</code></td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# show udld 1/0/0</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>exit</code></td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>

**Resetting Disabled UDLD on Ports With EVC Configured**

**SUMMARY STEPS**

1. `udld reset`

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>interface type/ slot/ port</code></td>
<td>Selects the LAN port to configure.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# gigethernet 1/0/0</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>`{udld port</td>
<td>no udld port } disable`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# udld port disable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# no udld port disable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>This command is supported only on fiber-optic LAN ports.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>show udld type/ slot/ port</code></td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# show udld 1/0/0</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>exit</code></td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>
DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>udld reset</strong></td>
<td>Resets all the LAN ports disabled by UDLD.</td>
</tr>
</tbody>
</table>

Example

This example displays the global configuration values at router 1:

Router(config)#udld enable

This example displays the ESM20 port at router 1:

Router(config)# interface gi 2/0/1
Router(config-if)# udld port aggressive
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# rewrite ingress tag translate 1-to2 dot1q 5 second-dot1q 5 symmetric
Router(config-if-srv)# bridge-domain 100

This example displays the configuration for a port that is part of a port channel:

Router(config)# interface Port-channel1
Router(config-if)# no ip address
Router(config-if)# service instance 1 ethernet
Router(config-if)# encapsulation untagged
Router(config-if)# bridge-domain 100

Router(config)# interface GigabitEthernet3/0/13
Router(config-if)# ip arp inspection limit none
Router(config-if)# no ip address
Router(config-if)# udld port aggressive
Router(config-if)# no mls qos trust
Router(config-if)# channel-group 1 mode on

Verification

Use the **show udld** and **show udld interface** commands to verify the UDLD configuration:

Router(config)# show udld gi 3/0/13
Interface Gi1/3
---Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5
Entry 1
---
Expiration time: 37
Cache Device index: 1
Current neighbor state: Bidirectional
Device ID: 011932118C0
Configuring Unidirectional Link Detection (UDLD) on Ports with EVCs

Port ID: Gi1/1
Neighbor echo 1 device: 0FF71CA880
Neighbor echo 1 port: Gi1/3

Message interval: 15
Time out interval: 5
CDP Device name: rish2
Control Plane Protection on Non Access Subinterfaces

A router is segmented into three planes of operation, each with a clearly defined objective. The data plane to forward data packets, the control plane to route the data correctly, and the management plane to manage network elements.

The Cisco 7600 ES+ line card forwards any control plane traffic during data transmission to the route processor (RP). If there is a continuous stream of control packets to the Cisco 7600 router, all the packets are forwarded to the RP in the router. If the packet rate is high, the control packet flow consumes the processing capacity, memory, buffers and other critical system resources, and the RP functionality is impacted. Control Plane Protection (COPP) is a mechanism to control the traffic destined to the RP from non access sub interfaces of the ES+ line card using QoS policies.

COPP is already supported on access sub interfaces and the main interfaces. Effective from Cisco IOS release 15.1(2)S, COPP on non access sub interfaces is also supported on the ES+ line card.

Restrictions and Usage Guidelines

Follow these restrictions and guidelines for configuring COPP on a non access subinterface is given as follows:

- Only the protocols ARP, DHCP, Ethernet Operations Administration and Maintenance (EOAM) and PPPoE support COPP.
- The total number of interfaces with COPP on an ES+ line card is 16000.
- If hardware assisted call admission control (CAC) is configured, COPP takes precedence over the CAC for PPPoE and DHCP control packets including FSOL.
- Packets Per Second (PPS) mode of traffic policing is not supported.

Configuring COPP on a Non Access Subinterface

Complete these steps to configure COPP on a non access subinterface.

Summary Steps

1. enable
2. configure terminal
3. class-map match-all class-map-name
4. match protocol protocol-name
5. match subscriber access
6. policy-map policy-map-name
7. class class-name
8. police cir cir-value
9. control-plane user-type access
10. service-policy input policy-map-name
11. interface type number
12. `encapsulation dot1q vlan-id`
13. `ip address ip-address mask`
14. `ip subscriber l2-connected`
15. `initiator { dhcp | static | unclassified }
16. `end`

**Detailed Steps**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router# enable</code></td>
</tr>
<tr>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 3** | class-map match-all `class-map-name`
| Example: | `Router(config)# class-map match-all cmap` |
| Enables class map configuration mode used to create a traffic class. |
| **Step 4** | match protocol `protocol-name`
| Example: | `Router(config-cmap)# match protocol arp` |
| Specifies the match criteria for a class-map. |
| **Step 5** | match subscriber access
| Example: | `Router(config-cmap)# match subscriber access` |
| Enables ISG COPP. |
| **Step 6** | policy-map `policy-map-name`
| Example: | `Router(config-cmap)# policy-map pmap` |
| Creates or modifies a control policy map, which is used to define a control policy, and enters the control policy map configuration mode. |
| **Step 7** | class `class-name`
| Example: | `Router(config-pmap)# class cmap` |
| Enters class map configuration mode, which is used to associate a service policy with a class. `class-name` - Name of a service policy class. The name can contain up to 40 alphanumeric characters. |
### Step 8
`police cir cir-value`

**Example:**
```
Router(config-pmap-c)# police cir 30000
```

Specifies the committed information rate (CIR) value in bits per second.

- **cir-value** - The supported range is 500 to 30000.

### Step 9
`control-plane user-type access`

**Example:**
```
Router(config)# control-plane user-type access
```

Enters control-plane configuration mode.

### Step 10
`service-policy input policy-map-name`

**Example:**
```
Router(config-cp-user)# service-policy input pmap
```

Attaches a QoS service policy to the control-plane host subinterface.

### Step 11
`interface type number`

**Example:**
```
Router(config)# interface gigabit ethernet 1/1.1
```

Specifies an interface and enters the interface configuration mode.

### Step 12
`encapsulation dot1q vlan-id`

**Example:**
```
Router(config-subif)# encapsulation dot1q 400
```

Defines the matching criteria to map dot1Q ingress frames on an interface to the appropriate service instance.

- **vlan-id** - An integer in the range of 1 to 4094.

### Step 13
`ip address ip-address mask`

**Example:**
```
Router(config-subif)# ip-address 1.1.1.1 255.255.255.0
```

Specifies an IP address for an interface.

### Step 14
`ip subscriber l2-connected`

**Example:**
```
Router(config-subif)# ip subscriber l2-connected
```

Specifies the type of IP subscriber to be hosted on the interface and enters the configuration mode.

### Step 15
`initiator (dhcp|static|unclassified)`
```
Router(config-subscriber)# initiator dhcp
```

Creates IP subscriber sessions upon receipt of the specified packet type.

- **dhcp** - IP session initiated by DHCP
- **static** - Static IP session initiated.
- **unclassified** - IP session initiated by unclassified traffic

### Step 16
`end`

Exits the global configuration mode.
Configuration Example

This example shows how to configure COPP on a non access sub interface. In the example, a class map cmap is created to specify the matching criteria. Then a policy map pmap that describes the policing to be applied, is created and the service policy is applied on the control plane user interface.

```
Router# enable
Router# configure terminal
Router(config)# class-map match-all cmap
Router(config-cmap)# match protocol dhcp
Router(config-cmap)# match subscriber access
Router(config-cmap)# policy-map pmap
Router(config-pmap)# class cmap
Router(config-pmap-c)# police cir 300000
Router(config)# control-plane user-type access
Router(config)# service-policy input pmap
Router(config)# interface gigabit ethernet 1/2.1
Router(config-subif)# encapsulation dot1q 400
Router(config-subif)# ip subscriber 12-connected
Router(config-subscriber)# initiator dhcp
Router(config-subscriber)# end
```

Verifying COPP on a Non Access Sub Interface

To verify the COPP on a non access subinterface, you can use the following commands in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform copp rate-limit protocol-name</td>
<td>Displays the number of conformed and exceeded bytes for each interface on the RP for the specified protocol.</td>
</tr>
<tr>
<td>show platform npc copp all</td>
<td>Displays the list of interfaces under each NP for which COPP is initiated in the line card.</td>
</tr>
<tr>
<td>show platform npc copp if_num detail</td>
<td>Displays the number of dropped packets and bytes for a given interface. First verify whether COPP is initiated on the interface with <code>show platform npc copp all</code> command and then use this command for the detailed output of a specific interface.</td>
</tr>
</tbody>
</table>

BFD Scale Improvement on ES+ Line Card for 7600

Bidirectional Forwarding Detection (BFD) scale improvement feature provides the functionality to offload a BFD session to an ES+ line card. BFD is a forwarding path failure detection protocol and reduces the overall network convergence time by sending rapid failure detection packets (messages) to the routing protocols for recalculating the routing table. Before Release 15.1(2)S, a BFD session was run as a software component on the Route Processor (RP). Hence, the performance of BFD was restricted to the capabilities of CPU and IOS on the RP on the Cisco 7600 Router. Effective failure detection requires BFD to run at high frequencies (using aggressive timers as low as 50ms), which was not possible because of CPU and IOS restrictions. Effective with Cisco IOS Release 15.1(2) S, apart from running a BFD session on the RP, you can also offload a BFD session to the ES+ line card based on specific conditions.
BFD Scale Improvement on ES+ Line Card for 7600

listed in the “Restrictions for BFD Scale Improvement” section on page 4-403.

Note
Effective with Cisco IOS Release 15.1(3)S2, BFD hardware offload is also supported for IPv6 addresses along with the IPv4 addresses.

Note
If you are running IPv4 and IPv6 sessions on an interface, you can enable or disable offloading IPv4 or IPv6 sessions using the `platform bfd disable-offload ipv4|ipv6` command. Once you enable or disable the offloading, it will effect all the hardware offload BFD sessions on the box.

Offloading a BFD session to an ES+ line card allows you to utilize the hardware resources and capabilities of an ES+ line card, and also distribute the processing load between RP and ES+ line card. It allows you to scale up to 2000 BFD sessions for each Cisco 7600 series router.

Note
You can scale up to 2000 sessions per chassis using static and OSPF routing protocol for IPv4 BFD sessions only. For scale number values for IPv6 BFD sessions, see the “Restrictions for BFD Scale Improvement” section on page 4-403 section.

Note
Effective with Cisco IOS Release 15.3(1)S, BFD hardware offload support for Hot Standby Router Protocol (HSRP) IPv4 is enabled on the Cisco 7600 series routers. The feature is enabled by default. To disable the feature on all interfaces, use the `no standby bfd all-interfaces` command. For more information on HSRP, see First Hop Redundancy Protocols Configuration Guide, Cisco IOS Release 15.2S. For configuration procedure, see “Configuring BFD Hardware Offload for HSRP IPv4” section on page 4-404.

**BFD Sessions Supported on RSP720 Versions**

Table 4-45 lists the number of IPv4 HW BFD sessions supported on various Route Switch Processor 720 (RSP 720) versions.

<table>
<thead>
<tr>
<th>Sessions</th>
<th>RSP720-3C-GE</th>
<th>RSP720-3CXL-GE</th>
<th>RSP720-3C-10GE</th>
<th>RSP720-3CXL-10GE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 Gb</td>
<td>2 Gb</td>
<td>1 Gb</td>
<td>2 Gb</td>
</tr>
<tr>
<td>OSPF BFD session scale number</td>
<td>1200</td>
<td>2000</td>
<td>1200</td>
<td>2000</td>
</tr>
</tbody>
</table>

1. The scale numbers are valid only for the HW BFD sessions on the box and not software BFD session.

Note
The number of HW BFD sessions supported for IGPs is same as what the individual IGPs can scale upto.

Table 4-46 lists the number of software BFD sessions supported on the various RSP720 versions.
Table 4-46 Software BFD Sessions Supported on the Various RSP720 Versions

<table>
<thead>
<tr>
<th>Timer</th>
<th>Supported Scale Number$^1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>50*3ms</td>
<td>128</td>
</tr>
<tr>
<td>999*3 ms</td>
<td>512</td>
</tr>
</tbody>
</table>

1. These numbers are valid only for the software BFD session on the box and not hardware BFD session.

**Note**

The number of BFD HSRP sessions supported for hardware and software are same as that of other clients.

Table 4-47 lists the delay timers for HSRP process initialization and preemption. Note that there is no fixed delay timers. The delay timers depend on the test-bed used. The timers listed in Table 4-47 are the ones used successfully in most of the scenarios.

Table 4-47 Delay Timers for HSRP IPv4 Process Initialization and Preemption

<table>
<thead>
<tr>
<th>Delay Timers</th>
<th>Minimum</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSRP process initialization</td>
<td>240</td>
<td>300</td>
</tr>
<tr>
<td>Preemption</td>
<td>240</td>
<td>300</td>
</tr>
</tbody>
</table>

Table 4-48 lists the number of sessions supported for each type of line card:

Table 4-48 Sessions Supported on Line Cards

<table>
<thead>
<tr>
<th>Line Card</th>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>7600-ES+40G3C</td>
<td>1000</td>
</tr>
<tr>
<td>7600-ES+40G3CXL</td>
<td>1000</td>
</tr>
<tr>
<td>7600-ES+20G3C</td>
<td>500</td>
</tr>
<tr>
<td>7600-ES+20G3CXL</td>
<td>500</td>
</tr>
<tr>
<td>7600-ES+4TG3C</td>
<td>1000</td>
</tr>
<tr>
<td>7600-ES+4TG3CXL</td>
<td>1000</td>
</tr>
<tr>
<td>7600-ES+2TG3C</td>
<td>500</td>
</tr>
<tr>
<td>7600-ES+2TG3CXL</td>
<td>500</td>
</tr>
<tr>
<td>76-ES+XT-2TG3C</td>
<td>500</td>
</tr>
<tr>
<td>76-ES+XT-2TG3CXL</td>
<td>500</td>
</tr>
<tr>
<td>76-ES+XT-4TG3C</td>
<td>1000</td>
</tr>
<tr>
<td>76-ES+XT-4TG3CXL</td>
<td>1000</td>
</tr>
<tr>
<td>76-ES+T-20G3CXL</td>
<td>500</td>
</tr>
<tr>
<td>76-ES+T-2TG3CXL</td>
<td>500</td>
</tr>
<tr>
<td>76-ES+T-40G3CXL</td>
<td>1000</td>
</tr>
<tr>
<td>76-ES+T-4TG3CXL</td>
<td>1000</td>
</tr>
</tbody>
</table>
## BFD Scale Improvement on ES+ Line Card for 7600

### SSO Behavior

A BFD session supports Stateful Switchover (SSO) when offloaded to the ES+ line card. For a BFD session running on the RP, the minimum supported transmit (Tx) and receive (Rx) timer value for SSO is 500ms. When a session is offloaded to an ES+ line card, the minimum supported Tx and Rx timer value for SSO is 50ms. Usually, a BFD session offloaded to an ES+ line card is not affected during an SSO. However, these scenarios may be observed:

- Session configuration changes from peer during SSO: The line card CPU does not detect the changed bits in the BFD packets during SSO.
- Network failure during SSO: This situation is not handled immediately. Once the SSO is over, the BFD changes due to network failure are handled.

### Restrictions for BFD Scale Improvement

The following restrictions apply for BFD scale improvement:

- A BFD session is supported on only RSP 720 and Supervisor 720 (SUP720), it is not supported on SUP32.
- Only BFD version 1 is supported.
- The BFD session can be offloaded only to an ES+ line card interface.
- Ensure that the ES+ Line Card interface configured with the BFD session is on global routing table. Effective from Cisco IOS Release 15.1(3)S and 15.1(2)S1, the interface with a BFD session can be on any Virtual Routing and Forwarding (VRF).
- Each network processor supports a total of 250 sessions distributed across its ports.
- BFD hardware offload is supported for IPv4 sessions with non-echo mode only.
- You can configure IPv4 and IPv6 sessions to co-exist on the router as well as the same interface.
- Only the single hop BFD hardware offload is supported for both the IPv4 and IPv6 sessions. BFD hardware offload supports either of these combinations for IPv4 and IPv6 sessions:
  - 1000 IPv6 BFD sessions and no IPv4 sessions.
  - 2000 IPv4 BFD sessions and no IPv6 sessions.
  - 500 IPv4 BFD sessions and 500 IPv6 sessions.
- BFD offload is supported only for the ethernet interface.
- Timer values for Tx and Rx should only be in multiples of 50 and should range between 50 and 950ms for both the local and remote BFD peer router.
- If the Failure in MPLS core does not converge before XC BFD timer expires, then the BFD session flaps.

### Line Card Sessions

<table>
<thead>
<tr>
<th>Line Card</th>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>76-ES+XC-20G3C</td>
<td>500</td>
</tr>
<tr>
<td>76-ES+XC-20G3CXL</td>
<td>500</td>
</tr>
<tr>
<td>76-ES+XC-40G3C</td>
<td>1000</td>
</tr>
<tr>
<td>76-ES+XC-40G3CXL</td>
<td>1000</td>
</tr>
</tbody>
</table>

---

76-ES+XC-20G3C 500  
76-ES+XC-20G3CXL 500  
76-ES+XC-40G3C 1000  
76-ES+XC-40G3CXL 1000  

---

Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide  
OL-16147-29  
4-403
BFD Tx jitter defined in RFC 5880 is not supported.

You cannot swap a BFD session between ES+ line card and IOS by changing the parameters when the BFD session is up and running. To swap a BFD session, you need to unconfigure and reconfigure the BFD session with the changed parameters.

BFD offload is not supported on port-channel orSVI interfaces.

In case of prolonged network instability and BFD session flaps, the session state may get stuck in the DOWN, INIT, or UP state. Unconfigure and reconfigure BFD to resolve this issue.

During line card OIR, the `show bfd neighbor detail` command may show discrepancy in the statistics counter. The statistics counter provide information about Rx or Tx counts for a particular session.

BFD supports 2000 sessions with OSPF as client on RSP. Example scenarios:
- All subinterfaces are configured as point to point.
- Four instances of OSPF are running with each instance supporting 500 BFD session.

Configure the symmetric slow timers to less than or equal to five seconds on both the ends to bring up the HW offloaded BFD sessions.

BFD supports a maximum of 10 IPv6 static route sessions on an interface.

Note
Irrespective of timers, BFD is not supported on the port-channel main interface and sub-interface with SUP 32.

Note
Effective with Cisco IOS Release 15.1 (3)S, BFD sessions are also supported on SUP720.

Note
If the local discriminator (LD) value is less than 8000, it signifies that the session is offloaded to hardware.

Configuring BFD Hardware Offload for 7600

The BFD offload functionality is enabled by default. You can configure BFD hardware offload on the route processor. For more information, see Bidirectional Forwarding Detection.

Configuring BFD Hardware Offload for HSRP IPv4

Complete these steps to configure BFD hardware offload for HSRP IPv4:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface gigabitethernet slot/port`
4. `encapsulation dot1q vlan-id`
5. `ip address ip-address`
6. `standby delay minimum min-seconds reload reload-seconds`
7. `standby version 2`
8. `standby [group-number] ip ip-address`
9. `standby [group-number] priority priority`
10. `standby [group-number] preempt [delay {minimum | reload | sync} seconds]`
11. `bfd interval milliseconds min_rx milliseconds multiplier multiplier-value`
12. `no bfd echo`
13. `end`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

   - enable

   **Example:**

     Router# enable

| **Step 2**

   - configure terminal

   **Example:**

     Router# configure terminal

| **Step 3**

   - interface gigabit ethernet slot/port

   **Example:**

     Router(config)# interface GigabitEthernet 2/1.2

| **Step 4**

   - encapsulation dot1q vlan-id

   **Example:**

     Router(config-subif)# encapsulation dot1q 3

| **Step 5**

   - ip address ip-address

   **Example:**

     Router(config-subif)# ip address 10.1.2.3 255.255.255.0

| **Step 6**

   - standby delay minimum min-seconds

   **Example:**

     Router(config-subif)# standby delay minimum 240 reload 300

| **Step 7**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 8**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 9**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 10**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 11**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 12**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 13**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 14**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 15**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 16**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 17**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 18**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 19**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 20**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 21**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 22**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 23**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 24**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 25**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 26**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 27**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 28**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1

| **Step 29**

   - standby version 2

   **Example:**

     Router(config-subif)# standby version 2

| **Step 30**

   - standby [group-number] ip [ip-address]

   **Example:**

     Router(config-subif)# standby 2 ip 10.1.2.1
### Configuration Example

This example shows how to configure BFD Hardware Offload for HSRP:

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1.2
Router(config-subif)# encapsulation dot1q 3
Router(config-subif)# ip address 10.1.2.3 255.255.255.0
Router(config-subif)# standby delay minimum 240 reload 300
Router(config-subif)# standby version 2
Router(config-subif)# standby 2 priority 110
Router(config-subif)# standby 2 preempt delay minimum 240 reload 300
Router(config-subif)# bfd interval 50 min_rx 50 multiplier 3
Router(config-subif)# no bfd echo
Router(config-subif)# end
```

### Verification

Use the `show bfd neighbors` command to verify the configuration:

```
Router# show bfd neighbors ipv4 10.1.2.4 details
IPv4 Sessions
NeighAddr          LD/RD   RH/RS State  Int
10.1.2.4            1/2152   Up      Up  Gi2/1.2
```

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong> standby [group-number] priority</td>
<td>Configures the HSRP priority.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)#standby 2 priority 110</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> standby [group-number] preempt</td>
<td>Configures the HSRP preemption and preemption delay.</td>
</tr>
<tr>
<td>[delay {minimum</td>
<td>reload</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)# standby 2</td>
<td></td>
</tr>
<tr>
<td>preempt delay minimum 240 reload 300</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> bfd interval milliseconds min_rx milliseconds multiplier multiplier-value</td>
<td>Sets the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)# bfd interval 50</td>
<td></td>
</tr>
<tr>
<td>min_rx 50 multiplier 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> no bfd echo</td>
<td>Disables BFD echo mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)# no bfd echo</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> end</td>
<td>Exits the interface or subinterface mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)# end</td>
<td></td>
</tr>
</tbody>
</table>
Information About BFD Deterministic Offload

Bidirectional Forwarding Detection (BFD) sessions can be hosted on hardware or software on the Ethernet Services Plus line cards on c7600 routers. The deterministic offload feature for BFD helps users decide where a BFD session is to be hosted. The introduction of the command `platform bfd offload-timer ms` ensures that if the session Tx timer that is configured is lower than, or equal to the offload-timer limit, the BFD session gets hosted on the hardware, if resources are available. The configuration of a session Tx timer that is higher than the offload timer limit ensures that the BFD session gets hosted in the software.

Key Points About BFD Deterministic Offload

- When the new command `platform bfd offload-timer ms` is applied or removed, the existing BFD sessions are unaffected. Only new sessions created thereafter show deterministic behavior. For the feature to affect existing sessions, the sessions need to be re-created.
- When the network processor limit (250 sessions per network processor) is reached, the newer BFD sessions created on that network processor go into an inactive state, and can be seen under the output for the `show bfd neighbors inactive` command. The following error message is displayed when the network processor is full: `BFD_HW_MAX_SESSIONS_EXCEEDED`. In the inactive state, performing a line card reload, supervisor switchover, or reload breaks the feature because these actions may trigger any of the inactive sessions to become active and vice versa.
- To avoid feature breakage and retain determinism, it is recommended that no sessions remain in the inactive state.
- Remove a session from the inactive state in the following ways:
  - Destroy the session.
  - Move the session to software by making it echo or authenticated, and then re-create it.
  - Increase the tx_timer of the session to a value that is greater than that of the offload timer.
  - Delete some hardware offload sessions to free network processor resources.
Configuring BFD Offload Timer

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `platform bfd offload-timer offload-timer`
4. `end`

**Detailed Steps**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>enable</code></td>
<td>Enables the privileged EXEC mode. If prompted, enter your password.</td>
</tr>
<tr>
<td>Example: <code>Router# enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2 <code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Router#configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3 <code>platform bfd offload-timer Tx-timer</code></td>
<td>Configures the offload timer limit, in milliseconds, above which hardware offload is denied.</td>
</tr>
<tr>
<td>Example: <code>Router(config)#platform bfd offload-timer 450</code></td>
<td></td>
</tr>
<tr>
<td>Step 4 <code>end</code></td>
<td>Exits the global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Router(config)#end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Example for BFD Offload Timer**

The following example shows a BFD Offload Timer configuration:

```
Router# enable
Router#configure terminal
Router(config)#platform bfd offload-timer 450
Router(config)#end
```

**BFD Template Support for IPv4 and IPv6**

The BFD template support allows you to configure BFD interval, multiplier, and echo configs. Effective with Cisco IOS Release 15.2(4)S, Cisco 7600 routers support BFD template for the IPv4, IPv6, and 10*3 timers.

**Restrictions for BFD Template Support**

Following restrictions apply to the BFD template support:

- You can assign the same template to multiple interfaces or subinterfaces to create separate sessions.
- When multiple sessions are associated with the same template, and if you change the template configuration, all the session parameters are updated.
If you add a new interval command to the existing template, it overwrites the existing command.

If you add a separate BFD template to an interface or subinterface already having a BFD template, the template associated with the interface or subinterface will be the one you added latest.

You can use the same BFD template for both IPv4 and IPv6 BFD sessions. You can also use separate templates for IPv4 and IPv6 BFD sessions.

For a single BFD session greater than or equal to 50 ms, you can either use a BFD template or a BFD interval command, but not both.

Restrictions for 10*3 BFD Timers

Following restrictions apply for the 10*3 BFD timers:

- The 10*3 BFD timers can be configured only by using the BFD template. However, the BFD template can be used for configuring 50 milliseconds of hardware offload sessions and software BFD sessions.
- The 10*3 BFD sessions are supported only on the hardware.
- A maximum of hundred 10*3 sessions are supported on an ES+ line card with a restriction of not more than 25 sessions per NP. See Table 4-49.

10*3 BFD sessions are supported on both IPv4 and IPv6 for the following clients:

- Static
- OSPF
- ISIS
- BGP
- EIGRP
- RIP, it is supported only for IPv4

BFD Sessions Supported for 10*3 Timers

Table 4-49 lists the number of HWO BFD sessions supported for 10*3 timers:

<table>
<thead>
<tr>
<th>Line Card</th>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>7600-ES+40G3C</td>
<td>100</td>
</tr>
<tr>
<td>7600-ES+40G3CXL</td>
<td>100</td>
</tr>
<tr>
<td>7600-ES+20G3C</td>
<td>50</td>
</tr>
<tr>
<td>7600-ES+20G3CXL</td>
<td>50</td>
</tr>
<tr>
<td>7600-ES+4TG3C</td>
<td>100</td>
</tr>
<tr>
<td>7600-ES+4TGCXL</td>
<td>100</td>
</tr>
<tr>
<td>7600-ES+2TG3C</td>
<td>50</td>
</tr>
<tr>
<td>7600-ES+2TGCX</td>
<td>50</td>
</tr>
<tr>
<td>76-ES+XT-2TG3C</td>
<td>50</td>
</tr>
<tr>
<td>76-ES+XT-2TG3CXL</td>
<td>50</td>
</tr>
</tbody>
</table>
Using the BFD Template

Complete these steps to use the BFD template:

**SUMMARY STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>bfd-template single-hop bfd-template-name</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>interval min-tx msec min-rx msec multiplier number</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>no echo</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>interface gigabitethernet slot/port.subinterface-number</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>bfd template bfd-template-name</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>exit</code></td>
<td></td>
</tr>
</tbody>
</table>

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password when prompted.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Configuration Examples

This example shows how to use a BFD template for configuring a 10ms session in hardware:

```
Router> enable
Router# configure terminal
Router(config)# bfd-template single-hop bfd10
Router(config-bfd)# interval min-tx 10 min-rx 10 multiplier 3
Router(config-bfd)# no echo
Router(config-bfd)# interface gigabitethernet3/1.1
Router(config-subintf)# bfd template bfd10
Router(config-subintf)# exit
```
This example shows how to use a BFD template for configuring a 50ms session in software:

```plaintext
Router(config-subintf)# bfd template bfd10
Router(config-subintf)# exit
```

This example shows how to verify the configuration:

```plaintext
Router# show bfd neighbor ipv6 3062::2 details
```

### Verification

This example shows how to verify the configuration:

```plaintext
Router(config)# bfd-template single-hop bfd50
Router(config-bfd)# interval min-tx 50 min-rx 50 multiplier 3
Router(config-bfd)# echo
Router(config)# interface gigabitethernet3/1.1
Router(config-subintf)# bfd template bfd50
Router(config-subintf)# exit
```

```plaintext
Verification

This example shows how to verify the configuration:

```plaintext
Router# show bfd neighbor ipv6 3062::2 details
```

IPV6 Sessions

<table>
<thead>
<tr>
<th>NeighAddr</th>
<th>LD/RD</th>
<th>RH/RS</th>
<th>State</th>
<th>Int</th>
</tr>
</thead>
</table>

Session state is UP and not using echo function.
Session Host: Hardware
OurAddr: 3062::1
Handle: 67
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 10000, MinRxInt: 10000, Multiplier: 3
Received MinRxInt: 10000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 10(0)
Rx Count: 22367
Tx Count: 22364
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: BGP CEF
Template: bfd10
Uptime: 00:03:46
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
C bit: 1
Multiplier: 3 - Length: 24
My Discr.: 67 - Your Discr.: 67
Min tx interval: 10000 - Min rx interval: 10000
Min Echo interval: 0
Troubleshooting BFD Hardware Offload

Table 4-50 provides troubleshooting solutions for the BFD scale improvement issues:
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| BFD session repeatedly goes up and down, or fails to come up. | Complete these steps and report the findings to the TAC team:  
  1. Use the `show bfd neighbor detail` command to verify whether or not a session is offloaded to IOS or hardware, and identify the local discriminator (LD) value.  
  2. Use the `show bfd summary` command to check the total number of sessions in both the up and down state.  
  3. Use the `show platform bfd session | include LD_no` command to verify whether or not the Route Processor Platform Dependent (RP PD) table contains the offloaded session.  
  4. Use the `attach linecard_no` command to attach to the line card console.  
  5. Use the `show platform npc bfd LD_no` command to verify the line card information for the offloaded sessions on the line card.  
  6. Use the `show bfd drops` command on the RP to verify the number of session drops. Use the command multiple times to check if the drop counter increments in value.  
   For further debugging, enable the debug CLIs with the console logging function disabled and use these commands on the RP:  
   - `debug platform bfd offload event` command to display the events related to the offloaded session.  
   - `debug platform bfd offload xdr` command to display the XDR (communication mechanism between RP/line card).  
   - `debug platform bfd offload error` command to display the error messages generated for the offloaded session.  
   Use these commands on the line card:  
   - `debug platform npc bfd event` command to display the line card PD events for the offloaded session.  
   - `debug platform npc bfd error` command to display the line card PD errors for the offloaded session.  
   - `debug platform npc bfd xdr` command to display the line card PD XDR events for the offloaded session.  

**Note** Contact TAC at this location: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html.
Unable to offload an existing session to hardware even though it already existed in the hardware. Usually, hardware offload reconfiguration include these steps:

1. Disable BFD interval using the `no bfd interval interval_val min_rx rx_value multiplier multiplier_val` command
2. Enable the BFD interval using the `bfd interval interval_val min_rx rx_value multiplier multiplier_val` command
3. Enable the non-echo mode using the `no bfd echo` command.

The BFD session is offloaded to IOS immediately after reconfiguring the bfd interval and before the `no bfd echo` command. Hence, the command to enable non-echo mode is not considered while initializing a session on the IOS.

Unable to offload a static route BFD session from IOS to ES+ line card.

Solution

Complete these steps to offload a static route BFD session from IOS to ES+ line card:

1. Use the `no bfd interval interval_val min_rx rx_value multiplier multiplier_val` command to remove BFD interval from the interface.
2. Use the `no ip route` command to remove the static route configuration. For example, use:
   
   router (config)# no ip route static bfd interface-type interface-number gateway
   
   (or)
   
   router (config)# no ip route [vrf vrf-name] prefix mask (ip-address | interface-type interface-number [ip-address]) [dhcp] [distance] [name next-hop-name] [permanent | track number] [tag tag]
3. Use the `bfd interval interval_val min_rx rx_value multiplier multiplier_val` command to configure the BFD interval on an interface.
4. Use the `no bfd echo` command to enable the BFD no-echo mode.
5. Use the `ip route` command to configure the static route configuration. For example, use:
   
   router (config)# ip route static bfd interface-type interface-number gateway
   
   (or)
   
   router (config)# ip route [vrf vrf-name] prefix mask (ip-address | interface-type interface-number [ip-address]) [dhcp] [distance] [name next-hop-name] [permanent | track number] [tag tag]
Ethernet Data Plane Loopback

The Ethernet Data Plane Loopback feature provides a means for remotely testing the throughput of an ethernet port. The feature helps in preventing truck roll (network outage) in remote locations during the initial service turn-up. In the Cisco 7600 series routers, the Ethernet Data Plane Loopback feature allows loopback of traffic per port or per port per VLAN. Up to two loopbacks per switch is allowed. It supports swapping of the MAC destination address and source address to allow a packet to traverse multiple switches between a test head and a test switch. The feature enables:

- Service turn-up
- Post service turn-up troubleshooting
- Out of service throughput testing

After you configure the per VLAN loopback, the remaining VLANs on the port continue to switch normally, allowing a non-disruptive loopback testing.

Restrictions for Ethernet Data Plane Loopback

- On ES+ and SIP-400 line cards, this feature is supported only on the service instance (with bridge-domain configured) on a physical interface.
- Facility and Terminal loopback is not supported in the same service instance.
- Only data packets are looped back. Loopback is not supported for control packets.
- Cisco 7600 series routers cannot be the traffic generator because the network processor on ES+ and SIP-400 line cards cannot generate traffic at line rate. For throughput measurement, connect the router to an external central test head which generates the traffic.
- On an ES+ line card, you cannot bypass the ingress policer, shaper, and the egress policer for the external loopback.
- You cannot apply egress shaper on an internal loopback.
- After you stop an internal loopback, you have to flush the mac-table entries learned for the loopback packets.
- You cannot enable loopback session and span at the same time for the configured service instance or port.
- Filtering option on the loopback is not supported. For instance, filtering with source MAC address, destination MAC address, and so on.
- We recommend you do not use the rewrite command under EVC.

Configuring the Ethernet Data Plane Loopback

Complete these steps to configure Ethernet Data Plane Loopback:

**SUMMARY STEPS**

| Step 1 | enable |
| Step 2 | configure terminal |
**Step 3** interface ethernet slot/port
**Step 4** service instance id ethernet
**Step 5** encapsulation dot1q vlan-id
**Step 6** bridge-domain bridge-id
**Step 7** ethernet loopback permit {external | internal}
**Step 8** exit
**Step 9** ethernet loopback start local interface interface-id [service instance id] {external | internal}

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# enable</td>
</tr>
<tr>
<td>Enables privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>- Enter your password when prompted.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface ethernet slot/port</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface gigabitEthernet 2/1</td>
</tr>
<tr>
<td>Specifies an interface and enters interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>service instance id ethernet</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# service instance 1 ethernet</td>
</tr>
<tr>
<td>Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>encapsulation dot1q vlan-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if-srv)# encapsulation dot1q 120</td>
</tr>
<tr>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>bridge-domain bridge-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if-srv)# bridge-domain 120</td>
</tr>
<tr>
<td>Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4      Configuring Layer 1 and Layer 2 Features

Ethernet Data Plane Loopback

To start the Ethernet Data Plane Loopback, perform the following step from privileged EXEC mode:

**Step 7**  
```
etherent loopback permit {external | internal}
```

**Example:**  
Router(config-if-srv)#etherent loopback permit external

**Step 8**  
```
exit
```

**Example:**  
Router(config-if-srv)#exit

To start the Ethernet Data Plane Loopback, perform the following step from privileged EXEC mode:

**Step 8**  
```
etherent loopback start local interface interface-id [service instance id] {external | internal}
```

**Example:**  
Router#etherent loopback start local interface gigabitethernet2/1 service instance 1 external

### Configuration Examples for Ethernet Data Plane Loopback

This example shows how to configure the Ethernet Data Plane Loopback:

```
router>enable
router#configure terminal
router(config)#interface gigabitEthernet 2/1
router(config-if)#service instance 1 etherent
router(config-if-srv)#encapsulation dot1q 120
router(config-if-srv)#bridge-domain 120
router(config-if-srv)#etherent loopback permit external
```

This example shows how to start an Ethernet Data Plane Loopback:

```
router>enable
router#etherent loopback start local interface gigabitEthernet 2/1 service instance 1 external
```

This is an intrusive loopback and the packets matched with the service will not be able to pass through. Continue? (yes/[no]):

Enter yes to continue.

### Verification

Use the `show ethernet loopback active` command to see the active sessions:

```
router>show ethernet loopback active
```
Ethernet Data Plane Loopback

Loopback Session ID : 1
Interface : GigabitEthernet2/1
Service Instance : 1
Direction : External
Time out(sec) : none
Status : on
Start time : 11:17:17.105 IST Wed Feb 13 2013
Time left : N/A
Dot1q/Dot1ad(s) : 120
Second-dot1q(s) :
Source Mac Address : Any
Destination Mac Address : Any
Ether Type : Any
Class of Service : Any
Llc-oui : Any

Total Active Session(s): 1
Total Internal Session(s): 0
Total External Session(s): 1

Use the show ethernet loopback permitted command to see the permitted loopbacks:

```
routet> show ethernet loopback permitted interface gigabitethernet1/1
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>SrvcInst</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet2/1</td>
<td>1</td>
<td>External</td>
</tr>
<tr>
<td>120</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GigabitEthernet2/1</td>
<td>1</td>
<td>Internal</td>
</tr>
<tr>
<td>120</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

--------------------------------------------------------------------------------