CONTENTS

CHAPTER 1

Configuring Pseudowire 1

Pseudowire Overview 1

Limitations 2

Circuit Emulation Overview 2

Structure-Agnostic TDM over Packet 3

Circuit Emulation Service over Packet-Switched Network 4

Asynchronous Transfer Mode over MPLS 6

Transportation of Service Using Ethernet over MPLS 6

Limitations 7

Configuring CEM 7

Configuration Guidelines and Restrictions 8

Configuring a CEM Group 8

Using CEM Classes 9

Configuring a Clear-Channel ATM Interface 11

Configuring CEM Parameters 11

Configuring Payload Size (Optional) 11

Setting the Dejitter Buffer Size 12

Setting an Idle Pattern (Optional) 12

Enabling Dummy Mode 12

Setting a Dummy Pattern 12

Shutting Down a CEM Channel 12

Configuring ATM 12

Configuring a Clear-Channel ATM Interface 12

Configuring ATM IMA 13

BGP PIC with TDM Configuration 16

Configuring Structure-Agnostic TDM over Packet (SAToP) 17
Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN)  18
Configuring a Clear-Channel ATM Pseudowire  20
Configuring an ATM over MPLS Pseudowire  21
  Configuring the Controller  21
  Configuring an IMA Interface  22
  Configuring the ATM over MPLS Pseudowire Interface  24
    Configuring 1-to-1 VCC Cell Transport Pseudowire  24
    Configuring N-to-1 VCC Cell Transport Pseudowire  26
    Configuring 1-to-1 VPC Cell Transport  26
    Configuring ATM AAL5 SDU VCC Transport  27
    Configuring a Port Mode Pseudowire  29
  Optional Configurations  30
Configuring an Ethernet over MPLS Pseudowire  31
Configuring Pseudowire Redundancy  33
Pseudowire Redundancy with Uni-directional Active-Active  35
Restrictions  36
Configuring Pseudowire Redundancy Active-Active—Protocol Based  37
Configuring the Working Controller for MR-APS with Pseudowire Redundancy Active-Active  37
Configuring the Protect Controller for MR-APS with Pseudowire Redundancy Active-Active  37
Verifying the Interface Configuration  37
Configuration Examples  38
  Example: CEM Configuration  39
  Example: BGP PIC with TDM Configuration  39
  Example: BGP PIC with TDM-PW Configuration  40
  Example: ATM IMA Configuration  41
  Example: ATM over MPLS  41
    Cell Packing Configuration Examples  41
    Cell Relay Configuration Examples  45
  Example: Ethernet over MPLS  48

CHAPTER 2

Automatic Protection Switching Configuration  51
Automatic Protection Switching  51
Inter Chassis Redundancy Manager  52
Limitations  52
Automatic Protection Switching Interfaces Configuration 53
Configuring a Working Interface 53
Configuring a Protect Interface 54
Configuring Other APS Options 55
Stateful MLPPP Configuration with MR-APS Inter-Chassis Redundancy 56
Monitoring and Maintaining APS 57

CHAPTER 3

Configuring Multi Router Automatic Protection Switching 59
Finding Feature Information 59
Restrictions for MR-APS 59
Information About MR-APS 60
Configuring MR-APS with HSPW-ICRM on a CEM interface 62
Verifying MR-APS 66
Configuration Examples for MR-APS 73
Configuring MR-APS on a POS interface 75
Configuring working node for POS MR-APS 75
Configuring protect node for POS MR-APS 78
Verifying MR-APS on POS interface 82
Configuration Examples for MR-APS on POS interface 83

CHAPTER 4

Hot Standby Pseudowire Support for ATM and TDM Access Circuits 85
Finding Feature Information 85
Prerequisites for Hot Standby Pseudowire Support for ATM and TDM Access Circuits 86
Restrictions for Hot Standby Pseudowire Support for ATM and TDM Access Circuits 86
Information About Hot Standby Pseudowire Support for ATM and TDM Access Circuits 87
How the Hot Standby Pseudowire Support for ATM and TDM Access Circuits Feature Works 87
Supported Transport Types 87
How to Configure Hot Standby Pseudowire Support for ATM and TDM Access Circuits 87
Configuring a Pseudowire for Static VPLS 88
Configuring Hot Standby Pseudowire Support for ATM and TDM Access Circuits 90
Verifying the Hot Standby Pseudowire Support for ATM and TDM Access Circuits Configuration 91
Configuration Examples for Hot Standby Pseudowire Support for ATM and TDM Access Circuits 93
CHAPTER 7

Transparent SONET or SDH over Packet (TSoP) Protocol 151

Prerequisites for TSoP 151
Restrictions for TSoP 151
Information About TSoP Smart SFP 152
Guidelines for TSoP Smart SFP 152
Configuring the Reference Clock 153
Configuration Examples for TSoP 154
Verification Examples 156
Verifying TSoP Smart SFP 156
Verifying Clock Source 157
Configuring Pseudowire

This chapter provides information about configuring pseudowire (PW) features on the router.

- Pseudowire Overview, on page 1
- Limitations, on page 7
- Configuring CEM, on page 7
- Configuring ATM, on page 12
- Configuring Structure-Agnostic TDM over Packet (SAToP), on page 17
- Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN), on page 18
- Configuring a Clear-Channel ATM Pseudowire, on page 20
- Configuring an ATM over MPLS Pseudowire, on page 21
- Configuring an Ethernet over MPLS Pseudowire, on page 31
- Configuring Pseudowire Redundancy, on page 33
- Pseudowire Redundancy with Uni-directional Active-Active, on page 35
- Restrictions, on page 36
- Configuring Pseudowire Redundancy Active-Active—Protocol Based, on page 37
- Configuring the Working Controller for MR-APS with Pseudowire Redundancy Active-Active, on page 37
- Configuring the Protect Controller for MR-APS with Pseudowire Redundancy Active-Active, on page 37
- Verifying the Interface Configuration, on page 37
- Configuration Examples, on page 38

Pseudowire Overview

The following sections provide an overview of pseudowire support on the router.

Effective Cisco IOS XE Release 3.18S:

- BGP PIC with TDM Pseudowire is supported on the ASR 900 router with RSP2 module.

- BGP PIC for Pseudowires, with MPLS Traffic Engineering is supported on the ASR 900 router with RSP1 and RSP2 modules.

Starting Cisco IOS XE Release 3.18.1SP, Pseudowire Uni-directional Active-Active is supported on the RSP1 and RSP3 modules.
Limitations

If you are running Cisco IOS XE Release 3.17S, the following limitation applies:

• BGP PIC with TDM Pseudowire is supported only on the ASR 900 router with RSP1 module.

If you are running Cisco IOS XE Release 3.17S and later releases, the following limitations apply:

• Channel associated signaling (CAS) is not supported on the T1/E1 and OC-3 interface modules on the router.
• BGP PIC is not supported for MPLS/LDP over MLPPP and POS in the core.
• BGP PIC is not supported for Multi-segment Pseudowire or Pseudowire switching.
• BGP PIC is not supported for VPLS and H-VPLS.
• BGP PIC is not supported for IPv6.
• If BGP PIC is enabled, Multi-hop BFD should not be configured using the `bfd neighbor fall-over` command.
• If BGP PIC is enabled, `neighbor ip-address weight` command should not be configured.
• If BGP PIC is enabled, `bgp nexthop trigger delay 6` under the `address-family ipv4` command and `bgp nexthop trigger delay 7` under the `address-family vpnv4` command should be configured. For information on the configuration examples for BGP PIC–TDM, see Example: BGP PIC with TDM-PW Configuration, on page 40.
• If BGP PIC is enabled and the targeted LDP for VPWS cross-connect services are established over BGP, perform the following tasks:
  • configure Pseudowire-class (pw-class) with encapsulation "mpls"
  • configure `no status control-plane route-watch` under the pw-class
  • associate the pw-class with the VPWS cross-connect configurations

If you are running Cisco IOS-XE 3.18S, the following restrictions apply for BGP PIC with MPLS TE for TDM Pseudowire:

• MPLS TE over MLPPP and POS in the core is not supported.
• Co-existence of BGP PIC with MPLS Traffic Engineering Fast Reroute (MPLS TE FRR) is not supported.

Circuit Emulation Overview

Circuit Emulation (CEM) is a technology that provides a protocol-independent transport over IP networks. It enables proprietary or legacy applications to be carried transparently to the destination, similar to a leased line.

The Cisco ASR 903 Series Router supports two pseudowire types that utilize CEM transport: Structure-Agnostic TDM over Packet (SAToP) and Circuit Emulation Service over Packet-Switched Network (CESoPSN). The following sections provide an overview of these pseudowire types.
Starting with Cisco IOS XE Release 3.15, the 32xT1/E1 and 8x T1/E1 interface modules support CEM CESoP and SATOP configurations with fractional timeslots.

With the 32xT1/E1 and 8xT1/E1 interface modules, the channelized CEM circuits configured under a single port (fractional timeslot) cannot be deleted or modified, unless the circuits created after the first CEM circuits are deleted or modified.

The following CEM circuits are supported on the 32xT1/E1 interface module:

**T1 mode**
- 192 CESOP circuits with fractional timeslot
- 32 CESOP circuit full timeslot
- 32 SATOP circuits.

**E1 mode**
- 256 CESOP circuit with fractional timeslot.
- 32 CESOP circuit full timeslot
- 32 SATOP circuit

### Structure-Agnostic TDM over Packet

SAToP encapsulates time division multiplexing (TDM) bit-streams (T1, E1, T3, E3) as PWs over public switched networks. It disregards any structure that may be imposed on streams, in particular the structure imposed by the standard TDM framing.

The protocol used for emulation of these services does not depend on the method in which attachment circuits are delivered to the provider edge (PE) devices. For example, a T1 attachment circuit is treated the same way for all delivery methods, including copper, multiplex in a T3 circuit, a virtual tributary of a SONET/SDH circuit, or unstructured Circuit Emulation Service (CES).

In SAToP mode the interface is considered as a continuous framed bit stream. The packetization of the stream is done according to IETF RFC 4553. All signaling is carried out transparently as a part of a bit stream. **Figure 1: Unstructured SAToP Mode Frame Format**, on page 3 shows the frame format in Unstructured SAToP mode.

*Figure 1: Unstructured SAToP Mode Frame Format*

<table>
<thead>
<tr>
<th>Encapsulation header</th>
<th>CE Control (4Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP (optional 12B)</td>
<td>CEoP Payload Bytes 1-N</td>
</tr>
</tbody>
</table>

**Table 1: SAToP T1 Frame: Payload and Jitter Limits**, on page 4 shows the payload and jitter limits for the T1 lines in the SAToP frame format.
Table 1: SAToP T1 Frame: Payload and Jitter Limits

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>960</td>
<td>320</td>
<td>10</td>
<td>192</td>
<td>64</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 2: SAToP E1 Frame: Payload and Jitter Limits, on page 4 shows the payload and jitter limits for the E1 lines in the SAToP frame format.

Table 2: SAToP E1 Frame: Payload and Jitter Limits

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1280</td>
<td>320</td>
<td>10</td>
<td>256</td>
<td>64</td>
<td>2</td>
</tr>
</tbody>
</table>

For instructions on how to configure SAToP, see Configuring Structure-Agnostic TDM over Packet (SAToP), on page 17.

Circuit Emulation Service over Packet-Switched Network

CESoPSN encapsulates structured TDM signals as PWs over public switched networks (PSNs). It complements similar work for structure-agnostic emulation of TDM bit streams, such as SAToP. Emulation of circuits saves PSN bandwidth and supports DS0-level grooming and distributed cross-connect applications. It also enhances resilience of CE devices due to the effects of loss of packets in the PSN.

CESoPSN identifies framing and sends only the payload, which can either be channelized T1s within DS3 or DS0s within T1. DS0s can be bundled to the same packet. The CESoPSN mode is based on IETF RFC 5086.

Each supported interface can be configured individually to any supported mode. The supported services comply with IETF and ITU drafts and standards.

Figure 2: Structured CESoPSN Mode Frame Format, on page 4 shows the frame format in CESoPSN mode.

Figure 2: Structured CESoPSN Mode Frame Format

Table 3: CESoPSN DS0 Lines: Payload and Jitter Limits, on page 5 shows the payload and jitter for the DS0 lines in the CESoPSN mode.
<table>
<thead>
<tr>
<th>DS0</th>
<th>Maximum Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</th>
<th>Minimum Payload</th>
<th>Maximum Jitter</th>
<th>Minimum Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>40</td>
<td>320</td>
<td>10</td>
<td>32</td>
<td>256</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>80</td>
<td>320</td>
<td>10</td>
<td>32</td>
<td>128</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>120</td>
<td>320</td>
<td>10</td>
<td>33</td>
<td>128</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>160</td>
<td>320</td>
<td>10</td>
<td>32</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>200</td>
<td>320</td>
<td>10</td>
<td>40</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>240</td>
<td>320</td>
<td>10</td>
<td>48</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>280</td>
<td>320</td>
<td>10</td>
<td>56</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>320</td>
<td>320</td>
<td>10</td>
<td>64</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>360</td>
<td>320</td>
<td>10</td>
<td>72</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>400</td>
<td>320</td>
<td>10</td>
<td>80</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>440</td>
<td>320</td>
<td>10</td>
<td>88</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>480</td>
<td>320</td>
<td>10</td>
<td>96</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>520</td>
<td>320</td>
<td>10</td>
<td>104</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>560</td>
<td>320</td>
<td>10</td>
<td>112</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>600</td>
<td>320</td>
<td>10</td>
<td>120</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>16</td>
<td>640</td>
<td>320</td>
<td>10</td>
<td>128</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>680</td>
<td>320</td>
<td>10</td>
<td>136</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>18</td>
<td>720</td>
<td>320</td>
<td>10</td>
<td>144</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>760</td>
<td>320</td>
<td>10</td>
<td>152</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>20</td>
<td>800</td>
<td>320</td>
<td>10</td>
<td>160</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>21</td>
<td>840</td>
<td>320</td>
<td>10</td>
<td>168</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>22</td>
<td>880</td>
<td>320</td>
<td>10</td>
<td>176</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>23</td>
<td>920</td>
<td>320</td>
<td>10</td>
<td>184</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>24</td>
<td>960</td>
<td>320</td>
<td>10</td>
<td>192</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>25</td>
<td>1000</td>
<td>320</td>
<td>10</td>
<td>200</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>26</td>
<td>1040</td>
<td>320</td>
<td>10</td>
<td>208</td>
<td>64</td>
<td>2</td>
</tr>
</tbody>
</table>
Asynchronous Transfer Mode over MPLS

An ATM over MPLS (AToM) PW is used to carry Asynchronous Transfer Mode (ATM) cells over an MPLS network. It is an evolutionary technology that allows you to migrate packet networks from legacy networks, while providing transport for legacy applications. AToM is particularly useful for transporting 3G voice traffic over MPLS networks.

You can configure AToM in the following modes:

- N-to-1 Cell—Maps one or more ATM virtual channel connections (VCCs) or virtual permanent connection (VPCs) to a single pseudowire.
- 1-to-1 Cell—Maps a single ATM VCC or VPC to a single pseudowire.
- Port—Maps a single physical port to a single pseudowire connection.

The Cisco ASR 903 Series Router also supports cell packing and PVC mapping for AToM pseudowires.

For more information about how to configure AToM, see Configuring an ATM over MPLS Pseudowire, on page 21.

Transportation of Service Using Ethernet over MPLS

Ethernet over MPLS (EoMPLS) PWs provide a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core network. EoMPLS PWs encapsulate Ethernet protocol data units (PDUs) inside MPLS packets and use label switching to forward them across an MPLS network. EoMPLS PWs are an evolutionary technology that allows you to migrate packet networks from legacy networks while providing transport for legacy applications. EoMPLS PWs also simplify provisioning, since the provider edge equipment only requires Layer 2 connectivity to the connected customer edge (CE) equipment. The Cisco ASR 903 Series Router implementation of EoMPLS PWs is compliant with the RFC 4447 and 4448 standards.

The Cisco ASR 903 Series Router supports VLAN rewriting on EoMPLS PWs. If the two networks use different VLAN IDs, the router rewrites PW packets using the appropriate VLAN number for the local network.
For instructions on how to create an EoMPLS PW, see Configuring an Ethernet over MPLS Pseudowire, on page 31.

Limitations

If you are running Cisco IOS XE Release 3.17S, the following limitation applies:

- BGP PIC with TDM Pseudowire is supported only on the ASR 900 router with RSP1 module.

If you are running Cisco IOS XE Release 3.17S and later releases, the following limitations apply:

- Channel associated signaling (CAS) is not supported on the T1/E1 and OC-3 interface modules on the router.
- BGP PIC is not supported for MPLS/LDP over MLPPP and POS in the core.
- BGP PIC is not supported for Multi-segment Pseudowire or Pseudowire switching.
- BGP PIC is not supported for VPLS and H-VPLS
- BGP PIC is not supported for IPv6.
- If BGP PIC is enabled, Multi-hop BFD should not be configured using the `bfd neighbor fall-over bfd` command.
- If BGP PIC is enabled, `neighbor ip-address weight weight` command should not be configured.
- If BGP PIC is enabled, `bgp nexthop trigger delay 6` under the `address-family ipv4` command and `bgp nexthop trigger delay 7` under the `address-family vpng4` command should be configured. For information on the configuration examples for BGP PIC–TDM, see Example: BGP PIC with TDM-PW Configuration, on page 40.
- If BGP PIC is enabled and the targeted LDP for VPWS cross-connect services are established over BGP, perform the following tasks:
  - configure Pseudowire-class (pw-class) with encapsulation "mpls"
  - configure `no status control-plane route-watch` under the pw-class
  - associate the pw-class with the VPWS cross-connect configurations

If you are running Cisco IOS-XE 3.18S, the following restrictions apply for BGP PIC with MPLS TE for TDM Pseudowire:

- MPLS TE over MLPPP and POS in the core is not supported.
- Co-existence of BGP PIC with MPLS Traffic Engineering Fast Reroute (MPLS TE FRR) is not supported.

Configuring CEM

This section provides information about how to configure CEM. CEM provides a bridge between a time-division multiplexing (TDM) network and a packet network, such as Multiprotocol Label Switching (MPLS). The
router encapsulates the TDM data in the MPLS packets and sends the data over a CEM pseudowire to the remote provider edge (PE) router. Thus, function as a physical communication link across the packet network.

The following sections describe how to configure CEM:

Note
Steps for configuring CEM features are also included in the Configuring Structure-Agnostic TDM over Packet (SAToP), on page 17 and Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN), on page 18 sections.

Configuration Guidelines and Restrictions
Not all combinations of payload size and dejitter buffer size are supported. If you apply an incompatible payload size or dejitter buffer size configuration, the router rejects it and reverts to the previous configuration.

Configuring a CEM Group
The following section describes how to configure a CEM group on the Cisco ASR 903 Series Router.

SUMMARY STEPS
1. enable
2. configure terminal
3. controller {t1 | e1} slot/subslot/port
4. cem-group group-number {unframed | timeslots timeslot}
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</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: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>controller {t1</td>
<td>e1} slot/subslot/port</td>
</tr>
<tr>
<td>Example: Router(config)# controller t1 1/0</td>
<td>• Use the slot and port arguments to specify the slot number and port number to be configured.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The slot number is always 0.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>cem-group group-number {unframed</td>
<td>timeslots timeslot}</td>
</tr>
</tbody>
</table>
Using CEM Classes

A CEM class allows you to create a single configuration template for multiple CEM pseudowires. Follow these steps to configure a CEM:

**Note**
The CEM parameters at the local and remote ends of a CEM circuit must match; otherwise, the pseudowire between the local and remote PE routers will not come up.

**Note**
You cannot apply a CEM class to other pseudowire types such as ATM over MPLS.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. class cem cem-class
4. payload-size size | dejitter-buffer buffer-size | idle-pattern pattern
5. exit
6. interface cem slot/subslot
7. exit
8. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Example:**

Router> enable

• Enter your password if prompted.

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

Router# configure terminal

| **Step 3** class cem cem-class | Creates a new CEM class |
|**Example:**

Router(config)# class cem mycemclass

| **Step 4** payload-size size | Enter the configuration commands common to the CEM class. This example specifies a sample rate, payload size, dejitter buffer, and idle pattern. |
|dejitter-buffer buffer-size| idle-pattern pattern|

|**Example:**

Router(config-cem-class)# payload-size 512

|**Example:**

Router(config-cem-class)# dejitter-buffer 10

|**Example:**

Router(config-cem-class)# idle-pattern 0x55

| **Step 5** exit | Returns to the config prompt. |

|**Example:**

Router(config-cem-class)# exit

| **Step 6** interface cem slot/subslot | Configure the CEM interface that you want to use for the new CEM class. |
|**Example:**

Router(config)# interface cem 0/0

**Note** The use of the `xconnect` command can vary depending on the type of pseudowire you are configuring.
### Configuring a Clear-Channel ATM Interface

#### Configuring CEM Parameters

The following sections describe the parameters you can configure for CEM circuits.

**Note**

The CEM parameters at the local and remote ends of a CEM circuit must match; otherwise, the pseudowire between the local and remote PE routers will not come up.

#### Configuring Payload Size (Optional)

To specify the number of bytes encapsulated into a single IP packet, use the `payload-size` command. The size argument specifies the number of bytes in the payload of each packet. The range is from 32 to 1312 bytes.

Default payload sizes for an unstructured CEM channel are as follows:

- E1 = 256 bytes
- T1 = 192 bytes
- DS0 = 32 bytes
Default payload sizes for a structured CEM channel depend on the number of time slots that constitute the channel. Payload size \( L \) in bytes, number of time slots \( N \), and packetization delay \( D \) in milliseconds have the following relationship: \( L = 8*N*D \). The default payload size is selected in such a way that the packetization delay is always 1 millisecond. For example, a structured CEM channel of 16xDS0 has a default payload size of 128 bytes.

The payload size must be an integer of the multiple of the number of time slots for structured CEM channels.

Setting the Dejitter Buffer Size

To specify the size of the dejitter buffer used to compensate for the network filter, use the dejitter-buffer size command. The configured dejitter buffer size is converted from milliseconds to packets and rounded up to the next integral number of packets. Use the size argument to specify the size of the buffer, in milliseconds. The range is from 1 to 32 ms; the default is 5 ms.

Setting an Idle Pattern (Optional)

To specify an idle pattern, use the [no] idle-pattern pattern1 command. The payload of each lost CESoPSN data packet must be replaced with the equivalent amount of the replacement data. The range for pattern is from 0x0 to 0xFF; the default idle pattern is 0xFF.

Enabling Dummy Mode

Dummy mode enables a bit pattern for filling in for lost or corrupted frames. To enable dummy mode, use the dummy-mode [last-frame | user-defined] command. The default is last-frame. The following is an example:

```bash
Router(config-cem)# dummy-mode last-frame
```

Setting a Dummy Pattern

If dummy mode is set to user-defined, you can use the dummy-pattern pattern command to configure the dummy pattern. The range for pattern is from 0x0 to 0xFF. The default dummy pattern is 0xFF. The following is an example:

```bash
Router(config-cem)# dummy-pattern 0x55
```

Shutting Down a CEM Channel

To shut down a CEM channel, use the shutdown command in CEM configuration mode. The shutdown command is supported only under CEM mode and not under the CEM class.

Configuring ATM

The following sections describe how to configure ATM features on the T1/E1 interface module:

Configuring a Clear-Channel ATM Interface

To configure the T1 interface module for clear-channel ATM, follow these steps:
**SUMMARY STEPS**

1. enable
2. configure terminal
3. controller {t1} slot/subslot/port
4. atm
5. 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>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 controller {t1} slot/subslot/port</td>
<td>Selects the T1 controller for the port you are configuring</td>
</tr>
<tr>
<td>Example:</td>
<td>(where slot/subslot identifies the location and /port identifies the port).</td>
</tr>
<tr>
<td>Router(config)# controller t1 0/3/0</td>
<td></td>
</tr>
<tr>
<td>Step 4 atm</td>
<td>Configures the port (interface) for clear-channel ATM. The router creates an ATM interface whose format is atm/slot/subslot/port.</td>
</tr>
<tr>
<td>Example:</td>
<td>Note The slot number is always 0.</td>
</tr>
<tr>
<td>Router(config-controller)# atm</td>
<td></td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# end</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

To access the new ATM interface, use the interface atm slot/subslot/port command.

This configuration creates an ATM interface that you can use for a clear-channel pseudowire and other features. For more information about configuring pseudowires, see Configuring Pseudowire, on page 1

**Configuring ATM IMA**

Inverse multiplexing provides the capability to transmit and receive a single high-speed data stream over multiple slower-speed physical links. In Inverse Multiplexing over ATM (IMA), the originating stream of ATM cells is divided so that complete ATM cells are transmitted in round-robin order across the set of ATM links. Follow these steps to configure ATM IMA on the Cisco ASR 903 Series Router.
ATM IMA is used as an element in configuring ATM over MPLS pseudowires. For more information about configuring pseudowires, see Configuring Pseudowire, on page 1

Note

The maximum ATM over MPLS pseudowires supported per T1/E1 interface module is 500.

To configure the ATM interface on the router, you must install the ATM feature license using the `license install atm` command. To activate or enable the configuration on the IMA interface after the ATM license is installed, use the `license feature atm` command.

For more information about installing licenses, see the Software Activation Configuration Guide, Cisco IOS XE Release 3S.

Note

You can create a maximum of 16 IMA groups on each T1/E1 interface module.

SUMMARY STEPS

1. enable
2. configure terminal
3. card type \{t1 | e1\} slot \[bay\]
4. controller \{t1 | e1\} slot/subslot/port
5. clock source internal
6. ima group group-number
7. exit
8. interface ATM slot/subslot/IMA group-number
9. no ip address
10. atm bandwidth dynamic
11. no atm ilmi-keepalive
12. exit

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>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 3</strong> card type {t1</td>
<td>e1} slot [bay]</td>
</tr>
<tr>
<td>Example:.Router(config)# card type e1 0 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> controller {t1</td>
<td>e1} slot/subslot/port</td>
</tr>
<tr>
<td>Example:.Router(config)# controller e1 0/0/4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> clock source internal</td>
<td>Sets the clock source to internal.</td>
</tr>
<tr>
<td>Example:.Router(config-controller)# clock source internal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ima group group-number</td>
<td>Assigns the interface to an IMA group, and set the scrambling-payload parameter to randomize the ATM cell payload frames. This command assigns the interface to IMA group 0.</td>
</tr>
<tr>
<td>Example:.Router(config-controller)# ima-group 0 scrambling-payload</td>
<td>Note: This command automatically creates an ATM0/IMAx interface.</td>
</tr>
<tr>
<td></td>
<td>To add another member link, repeat Step 3 to Step 6.</td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits the controller interface.</td>
</tr>
<tr>
<td>Example:.Router(config-controller)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> interface ATM{slot/subslot}IMA group-number</td>
<td>Specify the slot location and port of IMA interface group.</td>
</tr>
<tr>
<td>Example:.Router(config-if)# interface atm0/1/ima0</td>
<td>• slot—The location of the ATM IMA interface module.</td>
</tr>
<tr>
<td></td>
<td>• group-number—The IMA group.</td>
</tr>
<tr>
<td></td>
<td>The example specifies the slot number as 0 and the group number as 0.</td>
</tr>
</tbody>
</table>

*Note*
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>To explicitly configure the IMA group ID for the IMA interface, use the optional <code>ima group-id</code> command. You cannot configure the same IMA group ID on two different IMA interfaces; therefore, if you configure an IMA group ID with the system-selected default ID already configured on an IMA interface, the system toggles the IMA interface to make the user-configured IMA group ID the effective IMA group ID. The system toggles the original IMA interface to select a different IMA group ID.</td>
</tr>
</tbody>
</table>

**Step 9**

- `no ip address`
- **Example:**
  ```
  Router(config-if)# no ip address
  ```
  Disables the IP address configuration for the physical layer interface.

**Step 10**

- `atm bandwidth dynamic`
- **Example:**
  ```
  Router(config-if)# atm bandwidth dynamic
  ```
  Specifies the ATM bandwidth as dynamic.

**Step 11**

- `no atm ilmi-keepalive`
- **Example:**
  ```
  Router(config-if)# no atm ilmi-keepalive
  ```
  Disables the Interim Local Management Interface (ILMI) keepalive parameters.
  ILMI is not supported on the router starting with Cisco IOS XE Release 3.15S.

**Step 12**

- `exit`
- **Example:**
  ```
  Router(config)# exit
  ```
  Exits configuration mode.

**What to do next**

The above configuration has one IMA shorthaul with two member links (atm0/0 and atm0/1).

**BGP PIC with TDM Configuration**

To configure the TDM pseudowires on the router, see *Configuring CEM, on page 7*.

To configure BGP PIC on the router, see *IP Routing: BGP Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 900 Series)*.

See the configuration example, *Example: BGP PIC with TDM Configuration, on page 39*. 
Configuring Structure-Agnostic TDM over Packet (SAToP)

Follow these steps to configure SAToP on the Cisco ASR 903 Series Router:

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. controller [t1|e1] slot/sublot  
4. cem-group group-number {unframed | timeslots timeslot}  
5. interface cem slot/subslot  
6. xconnect ip_address encapsulation mpls  
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.  
Example: Router> enable  
- Enter your password if prompted. |
| **Step 2** configure terminal  
Example: Router# configure terminal | Enters global configuration mode. |
| **Step 3** controller [t1|e1] slot/sublot  
Example: Router(config-controller)# controller t1 0/4 | Configures the T1 or E1 interface. |
| **Step 4** cem-group group-number {unframed | timeslots timeslot}  
Example: Router(config-if)# cem-group 4 unframed | Assigns channels on the T1 or E1 circuit to the CEM channel. This example uses the unframed parameter to assign all the T1 timeslots to the CEM channel. |
| **Step 5** interface cem slot/subslot  
Example: Router(config)# interface CEM 0/4  
Example: Router(config-if)# no ip address  
Example: | Defines a CEM group. |
### Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN)

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `controller [e1 | t1] slot/subslot`
4. `cem-group group-number timeslots timeslots`
5. `exit`
6. `interface cem slot/subslot`
7. `xconnect ip_address encapsulation mpls`
8. `exit`
9. `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>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 6 xconnect ip_address encapsulation mpls</td>
<td>Binds an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 304 to the remote peer 10.10.2.204.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# xconnect 10.10.2.204 encapsulation mpls</td>
<td></td>
</tr>
<tr>
<td>Step 7 exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

#### What to do next

When creating IP routes for a pseudowire configuration, we recommend that you build a route from the cross-connect address (LDP router-id or loopback address) to the next hop IP address, such as `ip route 10.10.10.2 255.255.255.254 10.2.3.4`. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>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>3</td>
<td>controller [e1</td>
<td>t1] slot/subslot</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config)# controller e1 0/0</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>cem-group group-number timeslots timeslots</td>
<td>Assigns channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the timeslots parameter to assign specific timeslots to the CEM channel.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-controller)# cem-group 5 timeslots 1-24</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>exit</td>
<td>Exits controller configuration.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-controller)# exit</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>interface cem slot/subslot</td>
<td>Defines a CEM channel.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config)# interface CEM0/5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if-cem)# cem 5</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>xconnect ip_address encapsulation mpls</td>
<td>Binds an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 304 to the remote peer 10.10.2.204.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if)# xconnect 10.10.2.204 encapsulation mpls</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>exit</td>
<td>Exits the CEM interface.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-if-cem)# exit</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Clear-Channel ATM Pseudowire

To configure the T1 interface module for clear-channel ATM, follow these steps:

**SUMMARY STEPS**

1. `controller {t1} slot/subslot/port`
2. `atm`
3. `exit`
4. `interface atm slot/subslot/port`
5. `pvc vpi/vci`
6. `xconnect peer-router-id vcid {encapsulation mpls | pseudowire-class name}`
7. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Selects the T1 controller for the port you are configuring.</td>
</tr>
<tr>
<td><code>controller {t1} slot/subslot/port</code></td>
<td>Note: The slot number is always 0.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller t1 0/4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the port (interface) for clear-channel ATM. The router creates an ATM interface whose format is <code>atm/slot/subslot/port</code>.</td>
</tr>
<tr>
<td><code>atm</code></td>
<td>Note: The slot number is always 0.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# atm</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Returns you to global configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Selects the ATM interface in Step 2.</td>
</tr>
<tr>
<td><code>interface atm slot/subslot/port</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface atm 0/3/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures a PVC for the interface and assigns the PVC a VPI and VCI. Do not specify 0 for both the VPI and VCI.</td>
</tr>
<tr>
<td><code>pvc vpi/vci</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# pvc 0/40</td>
<td></td>
</tr>
</tbody>
</table>
Configuring an ATM over MPLS Pseudowire

ATM over MPLS pseudowires allow you to encapsulate and transport ATM traffic across an MPLS network. This service allows you to deliver ATM services over an existing MPLS network.

The following sections describe how to configure transportation of service using ATM over MPLS:

- Configuring the Controller, on page 21
- Configuring an IMA Interface, on page 22
- Configuring the ATM over MPLS Pseudowire Interface, on page 24

Configuring the Controller

SUMMARY STEPS

1. enable
2. configure terminal
3. card type {e1} slot/subslot
4. controller {e1} slot/subslot
5. clock source {internal | line}
6. ima-group group-number scrambling-payload
7. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</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&gt; 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>
</tbody>
</table>
### Configuring an IMA Interface

If you want to use ATM IMA backhaul, follow these steps to configure the IMA interface.

**Note**
You can create a maximum of 16 IMA groups on each T1/E1 interface module.

**SUMMARY STEPS**
1. `enable`
2. `configure terminal`
3. `interface ATM slot / IMA group-number`
4. `no ip address`

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# configure terminal</td>
<td>Configures IMA on an E1 or T1 interface.</td>
</tr>
</tbody>
</table>

**Step 3**
```
card type {e1} slot/subslot
```
Example:
```
Router(config)# card type e1 0 0
```

**Step 4**
```
controller {e1} slot/subslot
```
Example:
```
Router(config)# controller e1 0/4
```

**Step 5**
```
clock source {internal | line}
```
Example:
```
Router(config-controller)# clock source internal
```

**Step 6**
```
ima-group group-number scrambling-payload
```
Example:
```
Router(config-controller)# ima-group 0 scrambling-payload
```

If you want to configure an ATM IMA backhaul, use the `ima-group` command to assign the interface to an IMA group. For a T1 connection, use the `no-scrambling-payload` to disable ATM-IMA cell payload scrambling; for an E1 connection, use the `scrambling-payload` parameter to enable ATM-IMA cell payload scrambling.

The example assigns the interface to IMA group 0 and enables payload scrambling.

**Step 7**
```
exit
```
Example:
```
Router(config)# exit
```

Exits configuration mode.
## Configuring an IMA Interface

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1.   | enable           | Enables privileged EXEC mode.  
|      | Example:         | • Enter your password if prompted. |
|      | Router> enable   |         |
| 2.   | configure terminal | Enters global configuration mode. |
|      | Example:         |         |
|      | Router# configure terminal | |
| 3.   | interface ATM slot / IMA group-number | Specifies the slot location and port of IMA interface group. The syntax is as follows:  
|      | Example:         | • slot—The slot location of the interface module.  
|      | Router(config-controller)# interface atm0/ima0 | • group-number—The group number of the IMA group.  
|      | Example:         | The example specifies the slot number as 0 and the group number as 0.  
|      | Router(config-if)# | **Note** To explicitly configure the IMA group ID for the IMA interface, you may use the optional `ima group-id` command. You cannot configure the same IMA group ID on two different IMA interfaces; therefore, if you configure an IMA group ID with the system-selected default ID already configured on an IMA interface, the system toggles the IMA interface to make the user-configured IMA group ID the effective IMA group ID. At the same, the system toggles the original IMA interface to select a different IMA group ID. |
| 4.   | no ip address    | Enables the IP address configuration for the physical layer interface. |
|      | Example:         |         |
|      | Router(config-if)# no ip address | |
| 5.   | atm bandwidth dynamic | Specifies the ATM bandwidth as dynamic. |
|      | Example:         |         |
|      | Router(config-if)# atm bandwidth dynamic | |
| 6.   | no atm ilmi-keepalive | Enables the ILMI keepalive parameters. |
|      | Example:         |         |

---

**Time Division Multiplexing Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 900 Series)**

23
Purpose

Command or Action | Purpose
--- | ---
Router(config-if)# no atm ilmi-keepalive | Exits configuration mode.

Step 7
Exits configuration mode.

Example:
Router(config)# exit

What to do next

For more information about configuring IMA groups, see the Configuring ATM IMA, on page 13.

Configuring the ATM over MPLS Pseudowire Interface

You can configure ATM over MPLS is several modes according to the needs of your network. Use the appropriate section according to the needs of your network. You can configure the following ATM over MPLS pseudowire types:

- Configuring 1-to-1 VCC Cell Transport Pseudowire, on page 24—Maps a single VCC to a single pseudowire
- Configuring N-to-1 VCC Cell Transport Pseudowire, on page 26—Maps multiple VCCs to a single pseudowire
- Configuring 1-to-1 VPC Cell Transport, on page 26—Maps a single VPC to a single pseudowire
- Configuring ATM AAL5 SDU VCC Transport, on page 27—Maps a single ATM PVC to another ATM PVC
- Configuring a Port Mode Pseudowire, on page 29—Maps one physical port to a single pseudowire connection
- Optional Configurations, on page 30

Note
When creating IP routes for a pseudowire configuration, build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as ip route 10.10.2 255.255.255.255 10.2.3.4.

Configuring 1-to-1 VCC Cell Transport Pseudowire

A 1-to-1 VCC cell transport pseudowire maps one ATM virtual channel connection (VCC) to a single pseudowire. Complete these steps to configure a 1-to-1 pseudowire.

Note
Multiple 1-to-1 VCC pseudowire mapping on an interface is supported.

Mapping a Single PVC to a Pseudowire

To map a single PVC to an ATM over MPLS pseudowire, use the xconnect command at the PVC level. This configuration type uses AAL0 and AAL5 encapsulations. Complete these steps to map a single PVC to an ATM over MPLS pseudowire.
**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. interface ATM `slot / IMA group-number`  
4. `pvc slot/subslot l2transport`  
5. `encapsulation aal0`  
6. `xconnect router_ip_address vcid encapsulation mpls`  
7. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1 | **enable**  
**Example:**  
Router> enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| 2 | **configure terminal**  
**Example:**  
Router# configure terminal | Enters global configuration mode. |
| 3 | **interface ATM `slot / IMA group-number`**  
**Example:**  
Router(config-controller)# interface atm0/ima0 | Configures the ATM IMA interface. |
| 4 | **pvc slot/subslot l2transport**  
**Example:**  
Router(config-if-atm)# pvc 0/40 l2transport | Defines a PVC. Use the `l2transport` keyword to configure the PVC as a layer 2 virtual circuit. |
| 5 | **encapsulation aal0**  
**Example:**  
Router(config-if-atm-l2trans-pvc)# encapsulation aal0 | Defines the encapsulation type for the PVC. The default encapsulation type for the PVC is AAL5. |
| 6 | **xconnect router_ip_address vcid encapsulation mpls**  
**Example:**  
Router(config-if-atm-l2trans-pvc)# xconnect 1.1.1.1 40 encapsulation mpls | Binds an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding PVC 40 to the remote peer 1.1.1.1. |
| 7 | **end**  
**Example:**  
Router(config-if-atm-l2trans-pvp-xconn)# end | Exits configuration mode. |
Configuring N-to-1 VCC Cell Transport Pseudowire

An N-to-1 VCC cell transport pseudowire maps one or more ATM virtual channel connections (VCCs) to a single pseudowire. Complete these steps to configure an N-to-1 pseudowire.

Configuring 1-to-1 VPC Cell Transport

A 1-to-1 VPC cell transport pseudowire maps one or more virtual path connections (VPCs) to a single pseudowire. While the configuration is similar to 1-to-1 VPC cell mode, this transport method uses the 1-to-1 VPC pseudowire protocol and format defined in RFCs 4717 and 4446. Complete these steps to configure a 1-to-1 VPC pseudowire.

Note

Multiple 1-to-1 VCC pseudowire mapping on an interface is supported.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface ATM slot / IMA group-number
4. atm pvp vpi l2transport
5. xconnect peer-router-id vcid {encapsulation mpls
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</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&gt; 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>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface ATM slot / IMA group-number</td>
<td>Configures the ATM IMA interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-controller)# interface atm0/ima0</td>
<td></td>
</tr>
</tbody>
</table>
Configuring ATM AAL5 SDU VCC Transport

An ATM AAL5 SDU VCC transport pseudowire maps a single ATM PVC to another ATM PVC. Follow these steps to configure an ATM AAL5 SDU VCC transport pseudowire.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface ATM slot / IMA group-number`
4. `atm pvp vpi l2transport`
5. `encapsulation aal5`
6. `xconnect peer-router-id vcid encapsulation mpls`
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. |

---

### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>atm pvp vpi l2transport</td>
<td>Maps a PVP to a pseudowire.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Router(config-if-atm)# atm pvp 10 12transport
```

**Step 4**

**Example:**

```bash
Router(config-if-atm-l2trans-pvp)#
```

**Step 5**

**Example:**

```bash
Router(config-if-atm-l2trans-pvp)# xconnect
10.10.10.2 305 encapsulation mpls
```

**Step 6**

**Example:**

```bash
Router(config-if-atm-l2trans-pvp-xconn)# end
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>CONFIGURES THE ATM IMA INTERFACE.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface ATM <code>slot / IMA group-number</code></td>
<td>CONFIGURES THE ATM IMA INTERFACE.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# interface atm0/ima0</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)#</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> atm pvp vpi l2transport</td>
<td>CONFIGURES A PVC AND SPECIFIES A VCI OR VPI.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# pvc 0/12 l2transport</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if-atm-l2trans-pvc)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation aal5</td>
<td>SETS THE PVC ENCAPSULATION TYPE TO AAL5.</td>
</tr>
<tr>
<td><strong>Note</strong> You must use the AAL5 encapsulation for this transport type.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if-atm-l2trans-pvc)# encapsulation aal5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> xconnect peer-router-id vcid encapsulation mpls</td>
<td>BINDS AN ATTACHMENT CIRCUIT TO THE ATM IMA INTERFACE TO CREATE A PSEUDOWIRE. THIS EXAMPLE CREATES A PSEUDOWIRE BY BINDING THE ATM CIRCUIT 125 TO THE REMOTE PEER 25.25.25.25.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if-atm-l2trans-pvc)# xconnect 10.10.10.2 125 encapsulation mpls</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>EXITS CONFIGURATION MODE.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Port Mode Pseudowire

A port mode pseudowire allows you to map an entire ATM interface to a single pseudowire connection.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface ATM slot / IMA group-number`
4. `xconnect peer-router-id vcid encapsulation mpls`
5. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code>&lt;br&gt;Example: <code>Router&gt; enable</code></td>
<td>Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code>&lt;br&gt;Example: <code>Router# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>interface ATM slot / IMA group-number</code>&lt;br&gt;Example: <code>Router(config-controller)# interface atm0/ima0</code></td>
<td>Configures the ATM interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>xconnect peer-router-id vcid encapsulation mpls</code>&lt;br&gt;Example: <code>Router(config-if-atm-l2trans-pvc)# xconnect 10.10.10.2 125 encapsulation mpls</code></td>
<td>Binds an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 125 to the remote peer 10.10.10.2.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>exit</code>&lt;br&gt;Example: <code>Router(config)# exit</code></td>
<td>Exits configuration mode.</td>
</tr>
</tbody>
</table>
Optional Configurations

You can apply the following optional configurations to a pseudowire link.

Configuring Cell Packing

Cell packing allows you to improve the efficiency of ATM-to-MPLS conversion by packing multiple ATM cells into a single MPLS packet. Follow these steps to configure cell packing.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface ATM slot / IMA group-number`
4. `atm mcpt-timers timer1 timer2 timer3`
5. `atm pvp vpi l2transport`
6. `encapsulation aal5`
7. `cell-packing maxcells mcpt-timer timer-number`
8. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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 ATM slot / IMA group-number | Configures the ATM interface.  
Example:  
Router(config-controller)# interface atm0/ima0  
Example:  
Router(config-if)# |
| **Step 4** atm mcpt-timers timer1 timer2 timer3 | Defines the three Maximum Cell Packing Timeout (MCPT) timers under an ATM interface. The three independent MCPT timers specify a wait time before forwarding a packet.  
Example:  
Router(config-if)# atm mcpt-timers 1000 2000 3000 |
| **Step 5** atm pvp vpi l2transport | Configures a PVC and specifies a VCI or VPI.  
Example: |
### Configuring Pseudowire

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# <strong>pvc 0/12 l2transport</strong></td>
<td>Example:</td>
</tr>
<tr>
<td>Router(config-if-atm-l2trans-pvc)#</td>
<td>Sets the PVC encapsulation type to AAL5. <strong>Note</strong> You must use the AAL5 encapsulation for this transport type.</td>
</tr>
<tr>
<td><strong>Step 6</strong> encapsulation aal5</td>
<td>Example:</td>
</tr>
<tr>
<td>Router(config-if-atm-l2trans-pvc)# <strong>encapsulation aal5</strong></td>
<td>Specifies the maximum number of cells in PW cell pack and the cell packing timer. This example specifies 20 cells per pack and the third MCPT timer.</td>
</tr>
<tr>
<td><strong>Step 7</strong> cell-packing maxcells mcpt-timer timer-number</td>
<td>Example:</td>
</tr>
<tr>
<td>Router(config-if-atm-l2trans-pvc)# <strong>cell-packing 20 mcpt-timer 3</strong></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Example:</td>
</tr>
<tr>
<td>Router(config-if-atm-l2trans-pvc)# <strong>end</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring an Ethernet over MPLS Pseudowire

Ethernet over MPLS PWs allow you to transport Ethernet traffic over an existing MPLS network. The router supports EoMPLS pseudowires on EVC interfaces.

For more information about Ethernet over MPLS Pseudowires, see *Transportation of Service Using Ethernet over MPLS, on page 6.*

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **service instance number ethernet [name]**
5. **encapsulation [default | dot1q | priority-tagged | untagged]**
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. **exit**
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td><code>Router&gt; enable</code></td>
</tr>
<tr>
<td></td>
<td><strong>Enables privileged EXEC mode.</strong></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><strong>Example:</strong></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td></td>
<td><strong>Enters global configuration mode.</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# interface gigabitethernet 0/0/4</code></td>
</tr>
<tr>
<td></td>
<td><strong>Specifies the port on which to create the pseudowire and enters interface configuration mode. Valid interfaces are physical Ethernet ports.</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>service instance number ethernet [name]</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# service instance 2 ethernet</code></td>
</tr>
<tr>
<td></td>
<td><strong>Configure an EFP (service instance) and enter service instance configuration mode.</strong></td>
</tr>
<tr>
<td></td>
<td>• The <strong>number</strong> is the EFP identifier, an integer from 1 to 4000.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <strong>ethernet name</strong> is the name of a previously configured EVC. You do not need to use an EVC name in a service instance.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You can use service instance settings such as encapsulation, dot1q, and rewrite to configure tagging properties for a specific traffic flow within a given pseudowire session. For more information, see <a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ether/configuration/xe-3s/asr903/ce-%E9%86%9Ae-3s-asr903-book/ce-evc.html">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ether/configuration/xe-3s/asr903/ce-醚e-3s-asr903-book/ce-evc.html</a></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**encapsulation {default</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if-srv)# encapsulation dot1q 2</code></td>
</tr>
<tr>
<td></td>
<td><strong>Configure encapsulation type for the service instance.</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>default</strong>—Configure to match all unmatched packets.</td>
</tr>
<tr>
<td></td>
<td>• <strong>dot1q</strong>—Configure 802.1Q encapsulation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>priority-tagged</strong>—Specify priority-tagged frames, VLAN-ID 0 and CoS value of 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>• <strong>untagged</strong>—Map to untagged VLANs. Only one EFP per port can have untagged encapsulation.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>**xconnect peer-ip-address ve-id {encapsulation</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td><code>Binds the Ethernet port interface to an attachment circuit to create a pseudowire. This example uses virtual circuit (VC) 101 to uniquely identify the PW. Ensure that the remote VLAN is configured with the same VC.</code></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Router (config-if-srv)# xconnect 10.1.1.2 101 encapsulation mpls</td>
<td>Note When creating IP routes for a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as \texttt{ip route 10.10.10.2 255.255.255.255 10.2.3.4}.</td>
</tr>
</tbody>
</table>

**Step 7**

<table>
<thead>
<tr>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Pseudowire Redundancy

A backup peer provides a redundant pseudowire (PW) connection in the case that the primary PW loses connection; if the primary PW goes down, the Cisco ASR 903 Series Router diverts traffic to the backup PW. This feature provides the ability to recover from a failure of either the remote PE router or the link between the PE router and CE router.

*Figure 3: Pseudowire Redundancy, on page 33* shows an example of pseudowire redundancy.

*Figure 3: Pseudowire Redundancy*

![Pseudowire Redundancy Diagram](image)

**Note**

You must configure the backup pseudowire to connect to a router that is different from the primary pseudowire.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. pseudowire-class \{pw-class-name\}
4. encapsulation mpls
5. interface serial slot/subslot/port
6. backup delay enable-delay \{disable-delay | never\}
7. xconnect router-id encapsulation mpls
**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> pseudowire-class [pw-class-name]</td>
<td>Specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# pseudowire-class mpls</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> encapsulation mpls</td>
<td>Specifies MPLS encapsulation.</td>
</tr>
<tr>
<td>Example: Router(config-pw-class)# encapsulation mpls</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> interface serial slot/subslot/port</td>
<td>Enters configuration mode for the serial interface.</td>
</tr>
<tr>
<td>Example: Router(config)# interface serial0/0</td>
<td><strong>Note</strong> The slot number is always 0.</td>
</tr>
<tr>
<td><strong>Step 6</strong> backup delay enable-delay {disable-delay</td>
<td>never}</td>
</tr>
<tr>
<td>Example: Router(config)# backup delay 0 10</td>
<td>Where:</td>
</tr>
<tr>
<td></td>
<td>- enable-delay—Time before the backup PW takes over for the primary PW.</td>
</tr>
<tr>
<td></td>
<td>- disable-delay—Time before the restored primary PW takes over for the backup PW.</td>
</tr>
<tr>
<td></td>
<td>- never—Disables switching from the backup PW to the primary PW.</td>
</tr>
<tr>
<td><strong>Step 7</strong> xconnect router-id encapsulation mpls</td>
<td>Binds the Ethernet port interface to an attachment circuit to create a pseudowire.</td>
</tr>
<tr>
<td>Example: Router(config-if)# xconnect 10.10.10.2 101 encapsulation mpls</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> backup peer peer-router-ip-address vcid [pw-class pw-class name]</td>
<td>Defines the address and VC of the backup peer.</td>
</tr>
</tbody>
</table>
Pseudowire Redundancy with Uni-directional Active-Active

Pseudowire redundancy with uni-directional active-active feature configuration allows, pseudowires (PW) on both the working and protect circuits to remain in UP state to allow traffic to flow from the upstream. The `aps l2vpn-state detach` command and `redundancy all-active replicate` command is introduced to configure uni-directional active-active pseudowire redundancy.

In pseudowire redundancy Active-Standby mode, the designation of the active and standby pseudowires is decided either by the endpoint PE routers or by the remote PE routers when configured with MR-APS. The active and standby routers communicate via Protect Group Protocol (PGP) and synchronize their states. The PEs are connected to a Base Station Controller (BSC). APS state of the router is communicated to the Layer2 VPN, and is therby coupled with the pseudowire status.

![Figure 4: Pseudowire Redundancy with MR-APS](image)

BSC monitors the status of the incoming signal from the working and protect routers. In the event of a swithover at the BSC, the BSC fails to inform the PE routers, hence causing traffic drops.

With pseudowire redundancy Active-Active configuration, the traffic from the upstream is replicated and transmitted over both the primary and backup pseudowires. PE routers forwards the received traffic to the working and protect circuits. The BSC receives the same traffic on both the circuits and selects the better Rx link, ensuring the traffic is not dropped.
If the ASR 900 router is configured with the `aps l2vpn-state detach` command but, the ASR 901 router is not enabled with `redundancy all-active replicate` command, the protect PW is active after APS switchover. On the ASR 901 router, the PW state is UP and the data path status displays standby towards protect node. On an APS switchover on the ASR 900 router, the status is not communicated to ASR 901 router, and the VC data path state towards the protect node remains in the standby state.

### Restrictions

The following restrictions apply on the router:

- If the `aps l2vpn-state detach` command is enabled on the ASR 900 router, but the `redundancy all-active replicate` command not enabled on the ASR 901 router, the pseudowire status on the router displays UP, and the data path status for the protect node state displays Standby.

- After APS switchover on the ASR 900 router, the status is not communicated to ASR 901 router, and the virtual circuit data path state towards the protect node remains in the Standby state.

- The `aps l2vpn-state detach` command takes effect after a controller `shutdown` command, followed by a `no shutdown` command is performed. Alternately, the command can be configured when the controller is in shut state.

- The `status peer topology dual-homed` command in pseudowire-class configuration mode should not be configured on the ASR 900 router, irrespective of unidirectional or bidirectional mode. The command must be configured on the ASR 901 router.

- Traffic outages from the BSC to the BTS on PGP and ICRM failures at the working Active node, is same as the configured hold time.

Note: APS switchover may be observed on the protect node, when PGP failure occurs on the working Active node.
Convergence may be observed on performing a power cycle on the Active (whether on the protect or working) node. The observed convergence is same as the configured hold time.

**Configuring Pseudowire Redundancy Active-Active — Protocol Based**

```
encapsulation mpls
status peer topology dual-homed
controller E1 0/1
framing unframed
cem-group 8 unframed
```

**Configuring the Working Controller for MR-APS with Pseudowire Redundancy Active-Active**

The following configuration shows pseudowire redundancy active-active for MR-APS working controller:

```
controller sonet 0/1/0
aps group 2
aps adm
aps working 1
aps timers 1 3
aps l2vpn-state detach
aps hspw-icrm-grp 1
```

**Configuring the Protect Controller for MR-APS with Pseudowire Redundancy Active-Active**

Following example shows pseudowire redundancy active-active on MR-APS protect controller:

```
controller sonet 0/1/0
aps group 2
aps adm
aps unidirectional
aps protect 10 10.10.10.1
aps timers 1 3
aps l2vpn-state detach
aps hspw-icrm-grp 1
```

**Verifying the Interface Configuration**

You can use the following commands to verify your pseudowire configuration:
• show cem circuit—Displays information about the circuit state, administrative state, the CEM ID of the circuit, and the interface on which it is configured. If xconnect is configured under the circuit, the command output also includes information about the attached circuit.

Router# show cem circuit
?

<0-504>  CEM ID
detail   Detailed information of cem ckt(s)
interface  CEM Interface
summary   Display summary of CEM ckts

Router# show cem circuit

CEM Int.  ID  Line  Admin  Circuit  AC
--------------------------------------------------------------
CEM0/1/0  1  UP  UP  ACTIVE  --/--
CEM0/1/0  2  UP  UP  ACTIVE  --/--
CEM0/1/0  3  UP  UP  ACTIVE  --/--
CEM0/1/0  4  UP  UP  ACTIVE  --/--
CEM0/1/0  5  UP  UP  ACTIVE  --/--

• show cem circuit—Displays the detailed information about that particular circuit.

Router# show cem circuit 1

CEM0/1/0, ID: 1, Line State: UP, Admin State: UP, Ckt State: ACTIVE
Idle Pattern: 0xFF, Idle cas: 0x8, Dummy Pattern: 0xFF
Dejitter: 5, Payload Size: 40
Framing: Framed, (DS0 channels: 1-5)
Channel speed: 56
CEM Defects Set
Excessive Pkt Loss RatePacket Loss
Signalling: No CAS
Ingress Pkts: 25929  Dropped: 0
Egress Pkts: 0  Dropped: 0
CEM Counter Details
Input Errors: 0  Output Errors: 0
Pkts Missing: 25927  Pkts Reordered: 0
Misorder Drops: 0  JitterBuf Underrun: 1
Error Sec: 26  Severly Errored Sec: 26
Unavailable Sec: 5  Failure Counts: 1
Pkts Malformed: 0

• show cem circuit summary—Displays the number of circuits which are up or down per interface basis.

Router# show cem circuit summary

CEM Int.  Total  Active  Inactive
--------------------------------------
CEM0/1/0  5  5  0

• show running configuration—The show running configuration command shows detail on each CEM group.

Configuration Examples

The following sections contain sample pseudowire configurations.
Example: CEM Configuration

The following example shows how to add a T1 interface to a CEM group as a part of a SAToP pseudowire configuration. For more information about how to configure pseudowires, see Configuring Pseudowire, on page 1

Note

This section displays a partial configuration intended to demonstrate a specific feature.

controller T1 0/0/0
framing unframed
clock source internal
linecode b8zs
cablelength short 110
cem-group 0 unframed
interface CEM0/0/0
no ip address
cem 0
xconnect 18.1.1.1 1000 encapsulation mpls

Example: BGP PIC with TDM Configuration

CEM Configuration

pseudowire-class pseudowire1
encapsulation mpls
control-word
no status control-plane route-watch
controller SONET 0/2/3
description connected to CE2 SONET 4/0/0
framing sdh
clock source line
aug mapping au-4
au-4 1 tug-3 1
mode c-12
tug-2 1 e1 1 cem-group 1101 unframed
tug-2 1 e1 1 framing unframed
tug-2 1 e1 2 cem-group 1201 timeslots 1-10
au-4 1 tug-3 2
mode c-12
tug-2 5 e1 1 cem-group 1119 unframed
tug-2 5 e1 1 framing unframed
tug-2 5 e1 2 cem-group 1244 timeslots 11-20
au-4 1 tug-3 3
mode c-12
tug-2 5 e1 3 cem-group 1130 unframed
tug-2 5 e1 3 framing unframed
tug-2 7 e1 3 cem-group 1290 timeslots 21-30
interface CEM0/2/3
no ip address
cem 1101
Example: BGP PIC with TDM-PW Configuration

This section lists the configuration examples for BGP PIC with TDM and TDM–Pseudowire.

The below configuration example is for BGP PIC with TDM:

```
router bgp 1
neighbor 18.2.2.2 remote-as 1
neighbor 18.2.2.2 update-source Loopback0
neighbor 18.3.3.3 remote-as 1
neighbor 18.3.3.3 update-source Loopback0
!
address-family ipv4
  bgp additional-paths receive
  bgp additional-paths install
  bgp nexthop trigger delay 6
  network 17.5.5.5 mask 255.255.255.255
  neighbor 18.2.2.2 activate
  neighbor 18.2.2.2 send-community both
  neighbor 18.2.2.2 send-label
  neighbor 18.3.3.3 activate
  neighbor 18.3.3.3 send-community both
  neighbor 18.3.3.3 send-label
  exit-address-family
```
neighbor 18.3.3.3 activate
neighbor 18.3.3.3 send-community both
neighbor 18.3.3.3 send-label
neighbor 26.1.1.2 activate
exit-address-family
!
address-family vpnv4
  bgp nexthop trigger delay 7
  neighbor 18.2.2.2 activate
  neighbor 18.2.2.2 send-community extended
  neighbor 18.3.3.3 activate
  neighbor 18.3.3.3 send-community extended
exit-address-family

The below configuration example is for BGP PIC with TDM PW:

pseudowire-class pseudowire1
encapsulation mpls
control-word
no status control-plane route-watch
status peer topology dual-homed
!
Interface CEM0/0/0
cem 1
  xconnect 17.1.1.1 4101 encapsulation mpls pw-class pseudowire1

---

Example: ATM IMA Configuration

The following example shows how to add a T1/E1 interface to an ATM IMA group as a part of an ATM over MPLS pseudowire configuration. For more information about how to configure pseudowires, see Configuring Pseudowire, on page 1

Note
This section displays a partial configuration intended to demonstrate a specific feature.

controller t1 4/0/0
ima-group 0
clock source line
interface atm4/0/ima0
pvc 1/33 l2transport
encapsulation aal0
  xconnect 1.1.1.1 33 encapsulation mpls

Example: ATM over MPLS

The following sections contain sample ATM over MPLS configurations:

Cell Packing Configuration Examples

The following sections contain sample ATM over MPLS configuration using Cell Relay:
VC Mode

**CE 1 Configuration**

```conf
interface Gig4/3/0
no negotiation auto
load-interval 30
interface Gig4/3/0
ip address 20.1.1.1 255.255.255.0
interface ATM4/2/4
no shut
exit
interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 30.1.1.2 255.255.255.255 50.1.1.2
```

**CE 2 Configuration**

```conf
interface Gig8/8
no negotiation auto
load-interval 30
interface Gig8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
no shut
!
interface ATM6/2/1.10 point
ip address 50.1.1.2 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 20.1.1.2 255.255.255.255 50.1.1.1
```

**PE 1 Configuration**

```conf
interface Loopback0
ip address 192.168.37.3 255.255.255.255
!
interface ATM0/0/0
no shut
!
interface ATM0/0/0
atm mcpt-timers 150 1000 4095
interface ATM0/0/0.10 point
pvc 20/101 12transport
encapsulation aal0
cell-packing 20 mcpt-timer 1
xconnect 192.168.37.2 100 encapsulation mpls
!
interface Gig0/3/0
no shut
ip address 40.1.1.1 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
```
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

**PE 2 Configuration**

interface Loopback0
ip address 192.168.37.2 255.255.255.255
! interface ATM9/3/1
no shut
! interface ATM9/3/1
atm mcpt-timers 150 1000 4095
interface ATM9/3/1.10 point
pvc 20/101 l2transport
encapsulation aal0
cell-packing 20 mcpt-timer 1
xconnect 192.168.37.1 100 encapsulation mpls
!
interface Gig6/2
no shut
ip address 40.1.1.2 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

**VP Mode**

**CE 1 Configuration**

interface Gig4/3/0
no negotiation auto
load-interval 30
interface Gig4/3/0
ip address 20.1.1.1 255.255.255.0
interface ATM4/2/4
!
interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 30.1.1.2 255.255.255.255 50.1.1.2

**CE 2 Configuration**

!
interface Gig8/8
no negotiation auto
load-interval 30
interface Gig8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
no shut
interface ATM6/2/1.10 point
ip address 50.1.1.2 255.255.255.0
pvc 20/101
encapsulation aal5snap
ip route 20.1.1.2 255.255.255.255 50.1.1.1

PE 1 Configuration

interface Loopback0
ip address 192.168.37.3 255.255.255.255
interface ATM0/0/0
no shut
interface ATM0/0/0
atm mcpt-timers 150 1000 4095
interface ATM0/0/0.50 multipoint
atm pvp 20 12transport
cell-packing 10 mcpt-timer 1
xconnect 192.168.37.2 100 encapsulation mpls
interface Gig0/3/0
no shut
ip address 40.1.1.1 255.255.0.0
mpls ip
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

PE 2 Configuration

interface Loopback0
ip address 192.168.37.2 255.255.255.255
interface ATM9/3/1
no shut
interface ATM9/3/1
atm mcpt-timers 150 1000 4095
interface ATM9/3/1.50 multipoint
atm pvp 20 12transport
cell-packing 10 mcpt-timer 1
xconnect 192.168.37.3 100 encapsulation mpls
interface Gig6/2
no shut
ip address 40.1.1.2 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

Cell Relay Configuration Examples

The following sections contain sample ATM over MPLS configuration using Cell Relay:

VC Mode

**CE 1 Configuration**

```
! interface gigabitethernet4/3/0
no negotiation auto
load-interval 30
interface gigabitethernet4/3/0
ip address 20.1.1.1 255.255.255.0
!
interface ATM4/2/4
!
interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 30.1.1.2 255.255.255.255 50.1.1.2
!```

**CE 2 Configuration**

```
interface gigabitethernet8/8
no negotiation auto
load-interval 30
interface gigabitethernet8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
!
interface ATM6/2/1.10 point
ip address 50.1.1.2 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 20.1.1.2 255.255.255.255 50.1.1.1
```

**PE 1 Configuration**

```
! interface Loopback0
ip address 192.168.37.3 255.255.255.255
!```
interface ATM0/0/0
!
interface ATM0/0/0.10 point
pvc 20/101 l2transport
encapsulation aal0
xconnect 192.168.37.2 100 encapsulation mpls
!
interface gigabitethernet0/3/0
ip address 40.1.1.1 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.0.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

PE 2 Configuration
!
interface Loopback0
ip address 192.168.37.2 255.255.255.255
!
interface ATM9/3/1
!
interface ATM9/3/1.10 point
pvc 20/101 l2transport
encapsulation aal0
xconnect 192.168.37.3 100 encapsulation mpls
!
interface gigabitethernet6/2
ip address 40.1.1.2 255.255.0.0
mpls ip
!
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.0.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

VP Mode

CE 1 Configuration
!
interface gigabitethernet4/3/0
no negotiation auto
load-interval 30
interface gigabitethernet4/3/0
ip address 20.1.1.1 255.255.255.0
!
interface ATM4/2/4
!
interface ATM4/2/4.10 point
ip address 50.1.1.1 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 30.1.1.2 255.255.255.255 50.1.1.2

**CE 2 Configuration**

! interface gigabitethernet8/8
no negotiation auto
load-interval 30
interface gigabitethernet8/8
ip address 30.1.1.1 255.255.255.0
interface ATM6/2/1
!
interface ATM6/2/1.10 point
ip address 50.1.1.2 255.255.255.0
pvc 20/101
encapsulation aal5snap
!
ip route 20.1.1.2 255.255.255.255 50.1.1.1

**PE 1 Configuration**

interface Loopback0
ip address 192.168.37.3 255.255.255.255
!
!
interface ATM0/0/0
interface ATM0/0/0.50 multipoint
atm pvp 20 12transport
xconnect 192.168.37.2 100 encapsulation mpls
!
interface gigabitethernet0/3/0
ip address 40.1.1.1 255.255.0.0
mpls ip
!
mls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp graceful-restart
router ospf 1
network 40.1.0.0 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

**PE 2 Configuration**

interface Loopback0
ip address 192.168.37.2 255.255.255.255
!
!
interface ATM9/3/1
interface ATM9/3/1.50 multipoint
atm pvp 20 12transport
xconnect 192.168.37.3 100 encapsulation mpls
!
interface gigabitethernet6/2
ip address 40.1.1.2 255.255.0.0
mpls ip
Example: Ethernet over MPLS

PE 1 Configuration

! mpls label range 16 12000 static 12001 16000
mpls label protocol ldp
mpls ldp neighbor 10.1.1.1 targeted ldp
mpls ldp graceful-restart
multilink bundle-name authenticated
!
!
redundancy
mode sso
!
!
ip tftp source-interface GigabitEthernet0
!
!
interface Loopback0
  ip address 10.5.5.5 255.255.255.255
interface GigabitEthernet0/0/4
  no ip address
  negotiation auto
!
  service instance 2 ethernet
  encapsulation dot1q 2
  xconnect 10.1.1.1 1001 encapsulation mpls
!
  service instance 3 ethernet
  encapsulation dot1q 3
  xconnect 10.1.1.1 1002 encapsulation mpls
!
interface GigabitEthernet0/0/5
  ip address 172.7.7.77 255.0.0.0
  negotiation auto
mpls ip
mpls label protocol ldp
!
routerr ospf 1
  router-id 5.5.5.5
  network 5.5.5.5 0.0.0.0 area 0
  network 172.0.0.0 0.255.255.255 area 0
  network 10.33.33.33 0.0.0.0 area 0
  network 192.0.0.0 0.255.255.255 area 0
!

PE 2 Configuration

! mpls label range 16 12000 static 12001 16000
mpls label protocol ldp
mpls ldp neighbor 10.5.5.5 targeted ldp
mpls ldp graceful-restart
multilink bundle-name authenticated
!
!
redundancy
   mode sso
!
!
ip tftp source-interface GigabitEthernet0
!
interface Loopback0
   ip address 10.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0/4
   no ip address
   negotiation auto
!
service instance 2 ethernet
   encapsulation dot1q 2
   xconnect 10.5.5.5 1001 encapsulation mpls
!
service instance 3 ethernet
   encapsulation dot1q 3
   xconnect 10.5.5.5 1002 encapsulation mpls
!
interface GigabitEthernet0/0/5
   ip address 172.7.7.7 255.0.0.0
   negotiation auto
   mpls ip
   mpls label protocol ldp
!
routing ospf 1
   router-id 10.1.1.1
   network 10.1.1.1 0.0.0.0 area 0
   network 172.0.0.0 0.255.255.255 area 0
   network 10.33.33.33 0.0.0.0 area 0
   network 192.0.0.0 0.255.255.255 area 0
Configuring Pseudowire

Example: Ethernet over MPLS
Automatic Protection Switching Configuration

Automatic Protection Switching is not supported on the Cisco ASR 900 RSP3 module.

Automatic protection switching (APS) is a protection mechanism for SONET networks that enables SONET connections to switch to another SONET circuit when a circuit failure occurs. A protect interface serves as the backup interface for the working interface. When the working interface fails, the protect interface quickly assumes its traffic load.

• Automatic Protection Switching, on page 51
• Inter Chassis Redundancy Manager, on page 52
• Limitations, on page 52
• Automatic Protection Switching Interfaces Configuration, on page 53
• Configuring a Working Interface, on page 53
• Configuring a Protect Interface, on page 54
• Configuring Other APS Options, on page 55
• Stateful MLPPP Configuration with MR-APS Inter-Chassis Redundancy, on page 56
• Monitoring and Maintaining APS, on page 57

Automatic Protection Switching

The protection mechanism used for this feature is "1+1, Bidirectional, nonrevertive" as described in the Bellcore publication "TR-TSY-000253, SONET Transport Systems; Common Generic Criteria, Section 5.3." In the 1+1 architecture, there is one working interface (circuit) and one protect interface, and the same payload from the transmitting end is sent to both the receiving ends. The receiving end decides which interface to use. The line overhead (LOH) bytes (K1 and K2) in the SONET frame indicate both status and action.

The protect interface is configured with the IP address of the router that has the working interface. The APS Protect Group Protocol, which runs on top of UDP, provides communication between the process controlling the working interface and the process controlling the protect interface. Using this protocol, interfaces can be switched because of a router failure, degradation or loss of channel signal, or manual intervention. In bidirectional mode, the receive and transmit channels are switched as a pair.

Two SONET/SDH connections are required to support APS. In a telco environment, the SONET/SDH circuits must be provisioned as APS. You must also provision the operation (for example, 1+1), mode (for example, bidirectional), and revert options (for example, no revert). If the SONET/SDH connections are homed on two
separate routers (the normal configuration), an out of band (OOB) communications channel between the two routers needs to be set up for APS communication.

When configuring APS, we recommend that you configure the working interface first. Normal operation with 1+1 operation is to configure it as a working interface. Also configure the IP address of the interface being used as the APS OOB communications path.

APS uses Protect Group Protocol (PGP) between working and protect interfaces. The protect interface APS configuration should include an IP address of a loopback interface on the same router to communicate with the working interface using PGP. Using the PGP, POS interfaces can be switched in case of a degradation or loss of channel signal, or manual intervention. In bidirectional mode, the receive and transmit channels are switched as a pair.

In bidirectional APS the local and the remote connections negotiate the ingress interface to be selected for the data path. The egress interface traffic is not transmitted to both working and protect interfaces.

**Inter Chassis Redundancy Manager**

ICRM provides these capabilities for stateful MLPPP with MR-APS Inter-Chassis Redundancy implementation:

- Node health monitoring for complete node, PE, or box failure detection. ICRM also communicates failures to the applications registered with an ICRM group.
- Reliable data channels to transfer the state information.
- Detects active RP failure as node failure and notifies the controllers.

ICRM on the standby RP re-establishes the communication channel with peer node if the active RP fails.

For instructions on how to configure ICRM, see Stateful MLPPP Configuration with MR-APS Inter-Chassis Redundancy.

**Limitations**

- Starting Cisco IOS XE Release 3.11, APS is supported with CES.
- The APS group number range supported on the RSP2 module in `aps group-number` command is 1-191.
- APS is **not** supported with ATM.
- APS is **not** supported with IMA.
- APS is **not** supported with POS.
- APS supports HDLC, PPP, and MLPPP encapsulation.
- ATM Layer 2 AAL0 and AAL5 encapsulation types are supported
- APS is only supported on MLP and serial interfaces on the OC-3 interface module.
Automatic Protection Switching Interfaces Configuration

The following sections describe how to configure APS interfaces:

Note
We recommend that you configure the working interface before the protected interface in order to prevent the protected interface from becoming the active interface and disabling the working interface.

Note
For information about configuring optical interfaces for the first time, see the Cisco ASR 903 Series Router Chassis Configuration Guide.

Configuring a Working Interface

To configure a working interface, use the following commands beginning in global configuration mode.

Before you begin
To configure the controller in SDH mode, see Configuring Optical Interface Modules.

SUMMARY STEPS

1. controller sonet slot / port-adapter / port
2. aps group group-number acr
3. aps working circuit-number
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 controller sonet slot / port-adapter / port</td>
<td>Returns to controller configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller sonet 0/0/0</td>
<td></td>
</tr>
<tr>
<td>Step 2 aps group group-number acr</td>
<td>Configures the working interface group on a router. The APS group number must be greater than 1.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# aps group acr 1</td>
<td></td>
</tr>
<tr>
<td>Step 3 aps working circuit-number</td>
<td>Configures this interface as a working interface. 1 is the only supported circuit-number value.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# aps working 1</td>
<td></td>
</tr>
</tbody>
</table>
**Configuring a Protect Interface**

To configure a protect interface, use the following commands beginning in global configuration mode.

**Before you begin**

To configure the controller in SDH mode, see Configuring Optical Interface Modules.

**SUMMARY STEPS**

1. `controller sonet slot / port-adapter / port`
2. `aps group group-number acr`
3. `aps protect circuit-number ip-address`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>controller sonet slot / port-adapter / port</code>&lt;br&gt;Example:&lt;br&gt;Router(config)# controller sonet 0/0/0</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>aps group group-number acr</code>&lt;br&gt;Example:&lt;br&gt;Router(config-if)# aps group acr 2</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>aps protect circuit-number ip-address</code>&lt;br&gt;Example:&lt;br&gt;Router(config-if)# aps protect 1 7.7.7.7</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code>&lt;br&gt;Example:&lt;br&gt;Router(config-if)# end</td>
</tr>
</tbody>
</table>
Configuring Other APS Options

To configure the other APS options, use any of the following optional commands in interface configuration mode.

**SUMMARY STEPS**

1. `aps authenticate string`
2. `aps force circuit-number`
3. `aps group group-number`
4. `aps lockout circuit-number`
5. `aps manual circuit-number`
6. `aps revert minutes`
7. `aps timers seconds1 seconds2`
8. `aps unidirectional`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>(Optional) Configures the authentication string that the router uses to authenticate PGP message exchange between protect or working routers. The maximum length of the string is eight alphanumeric characters. Spaces are not accepted.</td>
</tr>
<tr>
<td><code>aps authenticate string</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Router(config-if)# aps authenticate authstring</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>(Optional) Manually switches the specified circuit to a protect interface, unless a request of equal or higher priority is in effect. For example, if the protect interface is configured as circuit 1, use the <code>aps force 1</code> command to set the protect interface to active.</td>
</tr>
<tr>
<td><code>aps force circuit-number</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Router(config-if)# aps force 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> If you do not want the protect port to be active all the time, use <code>no aps force 1</code> command after using <code>aps force 1</code> command. Similarly for <code>aps force 0</code> use use <code>no aps force 0</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) Allows more than one protect/working interface group to be supported on a router.</td>
</tr>
<tr>
<td><code>aps group group-number</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Router(config-if)# aps group 2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Prevents a working interface from switching to a protect interface. For example, if the protect interface is configured as circuit 1, use the <code>aps lockout 1</code> command to prevent the protect interface from becoming active.</td>
</tr>
<tr>
<td><code>aps lockout circuit-number</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Router(config-if)# aps lockout 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Manually switches a circuit to a protect interface, unless a request of equal or higher priority is in effect. For</td>
</tr>
<tr>
<td><code>aps manual circuit-number</code></td>
<td>Example:</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router(config-if)# aps manual 0</code></td>
<td>example, if the working interface is configured as circuit 0, the command is applied as follows:</td>
</tr>
<tr>
<td></td>
<td>* The <code>aps manual 0</code> command activates the working interface</td>
</tr>
<tr>
<td></td>
<td>* The <code>aps manual 1</code> command activates the protect circuit.</td>
</tr>
<tr>
<td></td>
<td>Applying the <code>no</code> form of the command removes the configuration and stops the router from sending K1 and K2 bytes on the interface.</td>
</tr>
</tbody>
</table>

#### Step 6

- **aps revert minutes**

  **Example:**

  `Router(config-if)# aps revert 10`

  (Optional) Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.

#### Step 7

- **aps timers seconds1 seconds2**

  **Example:**

  `Router(config-if)# aps timers 1 5`

  (Optional) Specifies the following values:

  - `seconds1` — The time between hello packets.
  - `seconds2` — The time that the working interface can be down before the router switches to the protect interface.

#### Step 8

- **aps unidirectional**

  **Example:**

  `Router(config-if)# aps unidirectional`

  (Optional) Configures a protect interface for unidirectional mode.

### Example

```bash
Router# configure terminal
Router# interface gigabit ethernet 0/1/0
Router(config-if)# aps force 1
Router(config-if)# aps unidirectional
```

## Stateful MLPPP Configuration with MR-APS Inter-Chassis Redundancy

Monitoring and Maintaining APS

To provide information about system processes, the Cisco IOS software includes an extensive list of EXEC commands that begin with the word show, which, when executed, display detailed tables of system information. Following is a list of some of the common show commands for the APS feature.

To display the information described, use these commands in privileged EXEC mode.

- Use the `show aps` command to display information about APS.
- Use the `show controller sonet slot` command to display information about the controller port.
- Use the `show interfaces` command to display information about the interface.

For more information about these commands, see the *Cisco IOS Interface and Hardware Component Command Reference*. 
CHAPTER 3

Configuring Multi Router Automatic Protection Switching

Note

Multi Router Automatic Protection Switching is not supported on the Cisco ASR 900 RSP3 module.

The Multi Router Automatic Protection Switching (MR-APS) integration with hot standby pseudowire (HSPW) feature is a protection mechanism for Synchronous Optical Network (SONET) networks that enables SONET connections to switch to another SONET circuit when a circuit failure occurs. A protect interface serves as the backup interface for the working interface. When the working interface fails, the protect interface quickly assumes its traffic load.

- Finding Feature Information, on page 59
- Restrictions for MR-APS, on page 59
- Information About MR-APS, on page 60
- Configuring MR-APS with HSPW-ICRM on a CEM interface, on page 62
- Configuring MR-APS on a POS interface, on page 75

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for MR-APS

- Asynchronous Transfer Mode (ATM) port mode is not supported.
- An APS group number must be greater than zero.
- Revertive APS mode on the Circuit Emulation (CEM) interface is not supported.
• Starting with Cisco IOS XE Release 3.15, CEM MR-APS switchover does not occur on an RP SSO.
• HSPW group number other than the redundancy interchassis group number is not supported.
• Do not configure the backup delay value command if the MR-APS integration with HSPW feature is configured.
• Unconfiguring the mpls ip command on the core interface is not supported.
• The hspw force switch command is not supported.
• When you enable MRAPS 1+1 unidirectional mode, the PW status does not change for ASR 903 routers. But, the same behavior is not seen for ASR 901 routers. To overcome this issue, reload the ASR 901 router.
• Ensure to have both ASR 903 and ASR 901 routers configured with unidirectional configuration mode for MRAPS 1+1, else it results in a traffic drop.

Information About MR-APS

This feature enables interface connections to switch from one circuit to another if a circuit fails. Interfaces can be switched in response to a router failure, degradation or loss of channel signal, or manual intervention. In a multi router environment, the MR-APS allows the protected SONET interface to reside in a different router from the working SONET interface.

Service providers are migrating to ethernet networks from their existing SONET or SDH equipment to reduce cost. Any transport over MPLS (AToM) PWs help service providers to maintain their investment in time division multiplexing (TDM) network and change only the core from SONET or SDH to ethernet. When the service providers move from SONET or SDH to ethernet, network availability is always a concern. Therefore, to enhance the network availability, service providers use PWs.

The HSPW support for TDM access circuits (ACs) allow the backup PW to be in a hot-standby state, so that it can immediately take over if the primary PW fails. The present HSPW solution does not support ACs as part of the APS group. The PWs which are configured over the protected interface, remain in the standby state. MR-APS integration with an HSPW is an integration of APS with CEM TDM HSPW and improves the switchover time.

For more information on APS, see the Automatic Protection Switching Configuration.

In the example below, routers P1 and PE1 are in the same APS group G1, and routers P2 and PE2 are in the same APS group G2. In group G1, P1 is the working router and PE1 is the protected router. Similarly in group G2, P2 is the working router and PE2 is the protected router.

The MR-APS integration with HSPW deployment involves cell sites connected to the provider network using bundled T1/E1 connections. These T1/E1 connections are aggregated into the optical carrier 3 (OC3) link using the add-drop multiplexers (ADMs).
Failover Operations

MR-APS integration with HSPW feature handles the following failures:

- Failure 1, where the link between ADM and P1 goes down, or the connecting ports at ADM or P1 go down.
- Failure 2, where the router P1 fails.
- Failure 3, where the router P1 is isolated from the core.

In case of failure 1, where either port at the ADM goes down, or the port at the router goes down, or the link between ADM and router fails, the APS switchover triggers the pseudowires at the protect interface to become active. The same applies to failure 2 as well where the complete router fails over.

In case of failure 3, where all the links carrying primary and backup traffic lose the connection, a new client is added to the inter chassis redundancy manager (ICRM) infrastructure to handle the core isolation. The client listens to the events from the ICRM. Upon receiving the core isolation event from the ICRM, the client either initiates the APS switchover, or initiates the alarm based on the peer core isolation state. If APS switchover occurs, it changes the APS inactive interface to active and hence activates the PWs at the interface. Similarly, when core connectivity goes up based upon the peer core isolation state, it clears the alarms or triggers the
Configuring MR-APS with HSPW-ICRM on a CEM interface

To configure MR-APS integration with HSPW-ICRM on a CEM interface, complete the following steps:

**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. redundancy
8. interchassis group *group-id*
9. member ip *ip-address*
10. backbone interface slot/bay/port
11. exit
12. controller SONET slot/bay/port
13. framing [SDH | SONET]
14. clock source line
15. sts-1 *sts1-number*
16. mode vt-15
17. vtg *vtg_number* t1 *t1_line_number* cem-group *group-number* timeslots *time-slot-range*
18. exit
19. aps group *group_id*
20. aps [working | protect] *aps-group-number*
21. aps hspw-icrm-grp *group-number*
22. `exit`
23. `interface cem slot/bay/port`
24. `cem group-number`
25. `xconnect peer-ip-address vc_id pw-class pw-class-name`
26. `backup peer peer-id vc-id pw-class pw-class-name`
27. `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></td>
<td>Router&gt; <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></td>
<td>Router# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>pseudowire-class pw-class-name</code></td>
<td>Specifies the name of a PW class and enters PW class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>pseudowire-class hspw_aps</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# <code>pseudowire-class hspw_aps</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>encapsulation mpls</code></td>
<td>Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the PW.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>encapsulation mpls</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-pw-class)# <code>encapsulation mpls</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>status peer topology dual-homed</code></td>
<td>Enables the reflection of the attachment circuit status on both the primary and secondary PWs. This configuration is necessary if the peer PEs are connected to a dual-homed device.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>status peer topology dual-homed</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-pw-class)# <code>status peer topology dual-homed</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>exit</code></td>
<td>Exits PW class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>exit</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-pw-class)# <code>exit</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>redundancy</code></td>
<td>Enters the redundancy configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>redundancy</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# <code>redundancy</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>interchassis group group-id</code></td>
<td>Configures an interchassis group within the redundancy configuration mode and enters the interchassis redundancy mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>interchassis group 50</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-red)# <code>interchassis group 50</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>member ip ip-address</code></td>
<td>Configures the IP address of the peer member group.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>member ip 60.60.60.2</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-r-ic)# <code>member ip 60.60.60.2</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 10** backbone interface slot/bay/port | Specifies the backbone interface.  
  - *slot*—Chassis slot number, which is always 0.  
  - *bay*—Card interface bay number in a slot. The range is from 0 to 5.  
  - *port*—Port or interface number. The range is from 0 to 7 for Gigabit Ethernet. |
| **Example:**  
  Router(config-r-ic)# backbone interface  
  GigabitEthernet 0/2/3 |  |
| **Step 11** exit | Exits the redundancy mode. |
| **Example:**  
  Router(config-r-ic)# exit |  |
| **Step 12** controller SONET slot/bay/port | Selects and configures a SONET controller and enters controller configuration mode.  
  - *slot*—Chassis slot number, which is always 0.  
  - *bay*—Card interface bay number in a slot. The range is from 0 to 5.  
  - *port*—Port or interface number. The range is from 0 to 7 for Gigabit Ethernet. |
| **Example:**  
  Router(config)# controller SONET 0/5/2 |  |
| **Step 13** framing [SDH | SONET] | Configures the controller with framing type. SONET framing is the default option. |
| **Example:**  
  Router(config-controller)# framing SONET |  |
| **Step 14** clock source line | Sets the clocking for individual T1 or E1 links. |
| **Example:**  
  Router(config-controller)# clock source line |  |
| **Step 15** sts-1 stsl-number | Specifies the STS identifier. |
| **Example:**  
  Router(config-controller)# sts-1 1 |  |
| **Step 16** mode vt-15 | Specifies the STS-1 mode of operation. |
| **Example:**  
  Router(config-ctrlr-sts1)# mode vt-15 |  |
| **Step 17** vtg vtg_number t1 t1_line_number cem-group group-number timeslots time-slot-range | Creates a Circuit Emulation Services over Packet Switched Network circuit emulation (CESoPSN) CEM group.  
  - *vtg*—Specifies the VTG number from 1-7.  
  - *t1*—Specifies the T1 line.  
  - *t1_line_number*—Specifies the T1 line number. |
| **Example:**  
  Router(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24 |  |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>cem-group</strong>—Creates a circuit emulation (CEM) channel from one or more time slots of a T1 line.</td>
<td></td>
</tr>
<tr>
<td>• <strong>group-number</strong>—CEM identifier to be used for this group of time slots. For T1 ports, the range is from 0 to 23.</td>
<td></td>
</tr>
<tr>
<td>• <strong>timeslots</strong>—Specifies that a list of time slots is to be used as specified by the <strong>time-slot-range</strong> argument.</td>
<td></td>
</tr>
<tr>
<td>• <strong>time-slot-range</strong>—Specifies the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 18</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-ctrlr-sts1)# exit</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Exits from the STS configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 19</th>
<th><strong>aps group group_id</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-controller)# aps group 1</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures the APS group for CEM.</td>
</tr>
</tbody>
</table>

| Step 20 | **aps [working | protect] aps-group-number** |
|---------|-------------------------------------|
| **Example:** | Router(config-controller)# aps working 1 |
| **Purpose:** | Configures the APS group as working or protect interface. **Note** For MR-APS, one router must be configured as aps working 1 and the other router must be configured as aps protect 1. |

<table>
<thead>
<tr>
<th>Step 21</th>
<th><strong>aps hspw-icrm-grp group-number</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-controller)# aps hspw-icrm-group 1</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Associates the APS group to an ICRM group number.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 22</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-controller)# exit</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Ends the controller session and returns to the configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 23</th>
<th><strong>interface cem slot/bay/port</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface cem 0/5/2</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures a serial interface and enters the interface configuration mode <strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>slot</strong>—Chassis slot number, which is always 0.</td>
</tr>
<tr>
<td></td>
<td>• <strong>bay</strong>—Card interface bay number in a slot. The range is from 0 to 5.</td>
</tr>
<tr>
<td></td>
<td>• <strong>port</strong>—Port or interface number. The range is from 0 to 7 for Gigabit Ethernet.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 24</strong></td>
<td></td>
</tr>
<tr>
<td><code>cem group-number</code></td>
<td>Selects the CEM circuit (group) to configure a PW for.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# cem 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 25</strong></td>
<td></td>
</tr>
<tr>
<td><code>xconnect peer-ip-address vcid pw-class pw-class-name</code></td>
<td>Specifies the IP address of the peer PE router and the 32-bit virtual circuit identifier shared between the PEs at each end of the control channel.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if-srv)# xconnect 3.3.3.3 1 pw-class hspw_aps</td>
<td></td>
</tr>
<tr>
<td><strong>Step 26</strong></td>
<td></td>
</tr>
<tr>
<td><code>backup peer peer-id vc-id pw-class pw-class-name</code></td>
<td>Specifies a redundant peer for a PW virtual circuit.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if-srv)# backup peer 4.3.3.3 90 pw-class vpws</td>
<td></td>
</tr>
<tr>
<td><strong>Step 27</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns 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>

**Verifying MR-APS**

- Use the `show cem circuit [cem-group-id | interface {CEM | Virtual-CEM} slot/subslot/port cem-group-id | detail | summary]` command to display CEM statistics for the configured CEM circuits. If `xconnect` is configured under the circuit, the command output also includes information about the attached circuit.

Following is a sample output of the `show cem circuit` command to display the detailed information about CEM circuits configured on the router:

```
Router# show cem circuit

<table>
<thead>
<tr>
<th>CEM Int.</th>
<th>ID</th>
<th>Ctrlr</th>
<th>Admin</th>
<th>Circuit</th>
<th>AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEM0/5/2</td>
<td>1</td>
<td>UP</td>
<td>UP</td>
<td>Active</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>2</td>
<td>UP</td>
<td>UP</td>
<td>Active</td>
<td>UP</td>
</tr>
</tbody>
</table>
```
Following is a sample output of the `show cem circuit 0-504` command to display the detailed information about that particular circuit:

```
Router# show cem circuit 1

CEM0/5/2 , ID: 1, Line: UP, Admin: UP, Ckt: ACTIVE Controller state: up, T1/E1 state: up Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 192
Framing: Unframed
CEM Defects Set None
Signalling: No CAS
RTP: No RTP
Ingress Pkts: 151066 Dropped: 0
Egress Pkts: 151066 Dropped: 0

CEM Counter Details
Input Errors: 0 Output Errors: 0
Pkts Missing: 0 Pkts Reordered: 0
Misorder Drops: 0 JitterBuf Underrun: 0
Error Sec: 0 SeverlyErroredSec: 0
Unavailable Sec: 0 Failure Counts: 0
Pkts Malformed: 0 JitterBuf Overrun: 0
```

- Use the `show mpls ldp neighbor` command to display the status of Label Distribution Protocol (LDP) sessions:

```
Router# show mpls ldp neighbor

Peer LDP Ident: 17.3.3.3:0; Local LDP Ident 17.1.1.1:0
TCP connection: 17.3.3.3:13282 - 17.1.1.1:646
State: Oper; Msgs sent/rcvd: 466/209; Downstream
Up time: 00:23:50
LDP discovery sources:
   GigabitEthernet0/4/0 , Src IP addr: 11.11.11.2
   Targeted Hello 17.1.1.1 -> 17.3.3.3, active, passive
Addresses bound to peer LDP Ident:
   70.70.70.1 22.22.22.2 17.3.3.3 11.11.11.2
Peer LDP Ident: 17.4.4.4:0; Local LDP Ident 17.1.1.1:0
TCP connection: 17.4.4.4:24248 - 17.1.1.1:646
```
State: Oper; Msgs sent/rcvd: 209/205; Downstream
Up time: 00:23:40
LDP discovery sources:
GigabitEthernet0/4/2, Src IP addr: 33.33.33.2
Targeted Hello 17.1.1.1 -> 17.4.4.4, active, passive
Addresses bound to peer LDP Ident:
70.70.70.2 44.44.44.2 17.4.4.4 33.33.33.2
Peer LDP Ident: 17.2.2.2:0; Local LDP Ident 17.1.1.1:0
TCP connection: 17.2.2.2.32112 - 17.1.1.1.646
State: Oper; Msgs sent/rcvd: 45/44; Downstream
Up time: 00:23:38
LDP discovery sources:
GigabitEthernet0/4/4, Src IP addr: 60.60.60.2
Addresses bound to peer LDP Ident:
22.22.22.1 44.44.44.1 17.2.2.2 60.60.60.2

- Use the **show mpls l2 vc** command to display information related to a VC:

```bash
Router# show mpls l2 vc
```

<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>CEM0/5/2</td>
<td>SATOP T1 1</td>
<td>17.3.3.3</td>
<td>1001</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 2</td>
<td>17.3.3.3</td>
<td>1002</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 3</td>
<td>17.3.3.3</td>
<td>1003</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 19</td>
<td>17.3.3.3</td>
<td>1019</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 20</td>
<td>17.3.3.3</td>
<td>1020</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 21</td>
<td>17.3.3.3</td>
<td>1021</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 22</td>
<td>17.3.3.3</td>
<td>1022</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 23</td>
<td>17.3.3.3</td>
<td>1023</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 25</td>
<td>17.3.3.3</td>
<td>1025</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 43</td>
<td>17.3.3.3</td>
<td>1043</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 44</td>
<td>17.3.3.3</td>
<td>1044</td>
<td>UP</td>
</tr>
<tr>
<td>Local intf</td>
<td>Local circuit</td>
<td>Dest address</td>
<td>VC ID</td>
<td>Status</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>--------------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 45</td>
<td>17.3.3.3</td>
<td>1045</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 46</td>
<td>17.3.3.3</td>
<td>1046</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 65</td>
<td>17.3.3.3</td>
<td>1065</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 66</td>
<td>17.3.3.3</td>
<td>1066</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 67</td>
<td>17.3.3.3</td>
<td>1067</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 68</td>
<td>17.3.3.3</td>
<td>1068</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 69</td>
<td>17.3.3.3</td>
<td>1069</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 83</td>
<td>17.3.3.3</td>
<td>1083</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 84</td>
<td>17.3.3.3</td>
<td>1084</td>
<td>UP</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 1</td>
<td>17.4.4.4</td>
<td>4001</td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 2</td>
<td>17.4.4.4</td>
<td>4002</td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 3</td>
<td>17.4.4.4</td>
<td>4003</td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 4</td>
<td>17.4.4.4</td>
<td>4004</td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 5</td>
<td>17.4.4.4</td>
<td>4005</td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 6</td>
<td>17.4.4.4</td>
<td>4006</td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 7</td>
<td>17.4.4.4</td>
<td>4007</td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 8</td>
<td>17.4.4.4</td>
<td>4008</td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 27</td>
<td>17.4.4.4</td>
<td>4027</td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 28</td>
<td>17.4.4.4</td>
<td>4028</td>
<td></td>
</tr>
<tr>
<td>Local intf</td>
<td>Local circuit</td>
<td>Dest address</td>
<td>VC ID</td>
<td>Status</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>--------------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 29</td>
<td>17.4.4.4</td>
<td>4029</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 30</td>
<td>17.4.4.4</td>
<td>4030</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 31</td>
<td>17.4.4.4</td>
<td>4031</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 50</td>
<td>17.4.4.4</td>
<td>4050</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 51</td>
<td>17.4.4.4</td>
<td>4051</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 52</td>
<td>17.4.4.4</td>
<td>4052</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 53</td>
<td>17.4.4.4</td>
<td>4053</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 54</td>
<td>17.4.4.4</td>
<td>4054</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 73</td>
<td>17.4.4.4</td>
<td>4073</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 74</td>
<td>17.4.4.4</td>
<td>4074</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 75</td>
<td>17.4.4.4</td>
<td>4075</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 76</td>
<td>17.4.4.4</td>
<td>4076</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 77</td>
<td>17.4.4.4</td>
<td>4077</td>
<td></td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEM0/5/2</td>
<td>SATOP T1 83</td>
<td>17.4.4.4</td>
<td>4083</td>
<td></td>
</tr>
</tbody>
</table>
R-96-2011#sh cem circuit

```
<table>
<thead>
<tr>
<th>CEM Int. ID Ctrlr Admin Circuit</th>
<th>AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 UP UP Active UP</td>
<td>UP</td>
</tr>
<tr>
<td>2 UP UP Active UP</td>
<td>UP</td>
</tr>
<tr>
<td>3 UP UP Active UP</td>
<td>UP</td>
</tr>
<tr>
<td>83 UP UP Active UP</td>
<td>UP</td>
</tr>
<tr>
<td>84 UP UP Active UP</td>
<td>UP</td>
</tr>
</tbody>
</table>
```

• Use the `show mpls l2 vc vc-id detail` command to display detailed information related to the VC:

```
Router# show mpls l2 vc 1001 detail
```

Local interface: CEM0/5/2 up, line protocol up, SATOP T1 1 up
   Destination address: 17.3.3.3, VC ID: 1001, VC status: up
   Output interface: Gi0/4/0, imposed label stack {42}
   Preferred path: not configured
   Default path: active
   Next hop: 11.11.11.2
   Create time: 00:26:04, last status change time: 00:03:36
   Last label FSM state change time: 00:23:00
   Signaling protocol: LDP, peer 17.3.3.3:0 up
   Targeted Hello: 17.1.1.1 (LDP Id) -> 17.3.3.3, LDP is UP
   Graceful restart: configured and enabled
   Non stop routing: not configured and not enabled
   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 AC circuit status sent: No fault
   Last local PW i/f circ status rcvd: 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 182, remote 42
   Group ID: local 0, remote 0
   MTU: local 0, remote 0
   Remote interface description:
   Sequencing: receive disabled, send disabled
   Control Word: On (configured: autosense)
   SSO Descriptor: 17.3.3.3/1001, local label: 182
   Dataplane:
   SSM segment/switch IDs: 1278679/4262 (used), PWID: 1
   VC statistics:
   transit packet totals: receive 201616, send 201617
   transit byte totals: receive 41129664, send 40323400
   transit packet drops: receive 0, seq error 0, send 0
• Use the `show hspw-aps-icrm group group-id` command to display information about a specified HSPW APS group:

```
Router# show hspw-aps-icrm group 100
```

ICRM group id 100, Flags : My core isolated No, Peer core isolated No, State Connect
APS Group id 1 hw_if_index 33 APS valid:Yes
Total aps grp attached to ICRM group 100 is 1

• Use the `show hspw-aps-icrm all` command to display information about all HSPW APS and ICRM groups:

```
Router# show hspw-aps-icrm all
```

ICRM group id 100, Flags : My core isolated No, Peer core isolated No, State Connect
APS Group id 1 hw_if_index 33 APS valid:Yes
Total aps grp attached to ICRM group 100 is 1 ICRM group count attached to MR-APS HSPW feature is 1

• Use the `show redundancy interchassis` command to display information about interchassis redundancy group configuration:

```
Router# show redundancy interchassis
```

Redundancy Group 100 (0x64)
Applications connected: MR-APS with HSPW
Monitor mode: RW
member ip: 60.60.60.2 "R-222-2028", CONNECTED
  Route-watch for 60.60.60.2 is UP
  MR-APS with HSPW state: CONNECTED
backbone int GigabitEthernet0/4/0 : UP (IP)
backbone int GigabitEthernet0/4/2 : UP (IP)

ICRM fast-failure detection neighbor table
IP Address Status Type Next-hop IP Interface
========== ====== ==== =========== =========
60.60.60.2 UP RW

• Use the `show aps` command to display information about the current APS feature:

```
Router# show aps
```

SONET 0/5/2 APS Group 1: working channel 1 (Active) (HA)
Protect at 60.60.60.2
PGF timers (from protect): hello time=1; hold time=10
SONET framing
Remote APS configuration: (null)

• Use the `show xconnect all` command to display information about all Cross-Connect attachment circuits and PWs:

```
Router# show xconnect all
```

Legend: XC ST=Xconnect State S1=Segment1 State S2=Segment2 State
UP=Up DN=Down AD=Admin Down IA=Inactive
SB=Standby HS=Hot Standby RV=Recovering NH=No Hardware

Verifying MR-APS
Configuration Examples for MR-APS

The following example shows how to configure the MR-APS integration with HSPW on a CEM interface on the working router with framing mode as SONET on router P1:

RouterP1> enable
RouterP1# configure terminal
RouterP1(config)# pseudowire-class hspw_aps
RouterP1(config-pw-class)# encapsulation mpls
RouterP1(config-pw-class)# status peer topology dual-homed
RouterP1(config-pw-class)# exit
RouterP1(config)# redundancy
RouterP1(config-red)# interchassis group 1
RouterP1(config-r-ic)# member ip 14.2.0.2
RouterP1(config-r-ic)# backbone interface GigabitEthernet 0/1/0
RouterP1(config-r-ic)# backbone interface GigabitEthernet 0/1/1
RouterP1(config-r-ic)# exit
RouterP1(config)# controller SONET 0/1/0
RouterP1(config-controller)# framing sonet
RouterP1(config-controller)# clock source line
RouterP1(config-controller)# sts-1 1
RouterP1(config-ctrlr-sts1)# mode vt-15
RouterP1(config-ctrlr-sts1)# vtg 1 tl 1 cem-group 0 timeslots 1-24
RouterP1(config-ctrlr-sts1)# exit
RouterP1(config-controller)# aps group 3
RouterP1(config-controller)# aps working 1
RouterP1(config-controller)# aps hspw-icrm-grp 1
RouterP1(config-controller)# exit
RouterP1(config)# interface cem 0/1/0
RouterP1(config-if)# cem 0
RouterP1(config-if)# xconnect 3.3.3.3 1 encapsulation mpls pw-class hspw_aps
RouterP1(config-if)# backup peer 4.4.4.4 2 pw-class hspw_aps
The following example shows how to configure the MR-APS integration with HSPW on a CEM interface on the protect router with framing mode as SONET on router PE1:

```
RouterPE1> enable
RouterPE1# configure terminal
RouterPE1(config)# pseudowire-class hspw_aps
RouterPE1(config-pw-class)# encapsulation mpls
RouterPE1(config-pw-class)# status peer topology dual-homed
RouterPE1(config-pw-class)# exit
RouterPE1(config)# redundancy
RouterPE1(config-red)# interchassis group 1
RouterPE1(config-red)# member ip 14.2.0.1
RouterPE1(config-red)# backbone interface GigabitEthernet 0/1/0
RouterPE1(config-red)# backbone interface GigabitEthernet 0/1/1
RouterPE1(config-red)# exit
RouterPE1(config)# controller SONET 0/2/0
RouterPE1(config-controller)# framing sonet
RouterPE1(config-controller)# clock source line
RouterPE1(config-controller)# flag peer 3.3.3.3 3
RouterPE1(config-controller)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterPE1(config-controller)# exit
RouterPE1(config-controller)# aps group 3
RouterPE1(config-controller)# aps protect 1 14.2.0.2
RouterPE1(config-controller)# aps hspw-icrm-grp 1
RouterPE1(config-controller)# exit
RouterPE1(config)# interface cem 0/2/0
RouterPE1(config-if)# cem 0
RouterPE1(config-if)# xconnect 3.3.3.3 3 pw-class hspw_aps
RouterPE1(config-if)# backup peer 4.4.4.4 4 pw-class hspw_aps
RouterPE1(config-if)# exit
RouterPE1(config)# end
```

The following example shows how to configure the MR-APS integration with HSPW on a CEM interface on the working router with framing mode as SONET on router P2:

```
RouterP2> enable
RouterP2# configure terminal
RouterP2(config)# pseudowire-class hspw_aps
RouterP2(config-pw-class)# encapsulation mpls
RouterP2(config-pw-class)# status peer topology dual-homed
RouterP2(config-pw-class)# exit
RouterP2(config)# redundancy
RouterP2(config-red)# interchassis group 1
RouterP2(config-red)# member ip 14.6.0.2
RouterP2(config-red)# backbone interface GigabitEthernet 0/2/0
RouterP2(config-red)# backbone interface GigabitEthernet 0/2/1
RouterP2(config-red)# exit
RouterP2(config)# controller SONET 0/1/0
RouterP2(config-controller)# framing sonet
RouterP2(config-controller)# clock source line
RouterP2(config-controller)# sts-1 1
RouterP2(config-controller)# flag peer 1.1.1.1 1
RouterP2(config-controller)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterP2(config-controller)# exit
RouterP2(config-controller)# aps working 1
RouterP2(config-controller)# aps hspw-icrm-grp 1
RouterP2(config-controller)# exit
RouterP2(config)# interface cem 0/1/0
RouterP2(config-if)# cem 0
RouterP2(config-if)# xconnect 1.1.1.1 1 encapsulation mpls pw-class hspw_aps
```
Configuring MR-APS on a POS interface

The following section shows how to configure the MR-APS integration on a POS interface on the working node and protect node.

Configuring working node for POS MR-APS

To configure MR-APS working node for POS interface, complete the following steps:

SUMMARY STEPS

1. enable
2. configure terminal
3. exit
4. redundancy
5. interchassis group group-id
6. member ip ip-address
7. monitor peer bfd
8. exit
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  Example:  
  Router> enable |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  Router# configure terminal |
| **Step 3** exit | Exits PW class configuration mode.  
  Example:  
  Router(config-pw-class)# exit |
| **Step 4** redundancy | Enters the redundancy configuration mode.  
  Example:  
  Router(config)# redundancy |
| **Step 5** interchassis group *group-id* | Configures an interchassis group within the redundancy configuration mode and enters the interchassis redundancy mode.  
  Example:  
  Router(config-red)# interchassis group 50 |
| **Step 6** member ip *ip-address* | Configures the IP address of the peer member group.  
  Example:  
  Router(config-r-ic)# member ip 60.60.60.2 |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> monitor peer bfd</td>
<td>Enables BFD on the POS link.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-red)# monitor peer bfd</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits the redundancy mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-r-ic)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> controller SONET slot/bay/port</td>
<td>Selects and configures a SONET controller and enters controller configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller SONET 0/5/2</td>
<td></td>
</tr>
<tr>
<td>• slot—Chassis slot number, which is always 0.</td>
<td></td>
</tr>
<tr>
<td>• bay—Card interface bay number in a slot. The range is from 0 to 5.</td>
<td></td>
</tr>
<tr>
<td>• port—Port or interface number. The range is from 0 to 7 for Gigabit Ethernet.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> framing [SDH</td>
<td>SONET]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# framing SONET</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> clock source internal</td>
<td>Sets the clocking for individual E1 links.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# clock source internal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> sts-1 1-3POS</td>
<td>Specifies the STS identifier.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# sts-1 1-3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> exit</td>
<td>Exits from the STS configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-ctrlr-sts1)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> controller SONET slot/bay/port</td>
<td>Selects and configures a SONET controller and enters controller configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller SONET 0/5/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong> Shutdown</td>
<td>Shut down the controller before APS configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# Shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> aps group group_id</td>
<td>Configures the APS group for POS.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# aps group 1</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 17</td>
<td><strong>aps working</strong> <em>aps-group-number</em></td>
<td>Configures the APS group as working or protect interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Router(config-controller)# aps working 1</em></td>
<td></td>
</tr>
<tr>
<td>Step 18</td>
<td><strong>aps interchassis group</strong> <em>group-id</em></td>
<td>Configures an aps inter chassis group.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Router(config-red)# aps interchassis group 50</em></td>
<td></td>
</tr>
<tr>
<td>Step 19</td>
<td><strong>no shut</strong></td>
<td>Shut down the controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Router(config-controller)# no shut</em></td>
<td></td>
</tr>
<tr>
<td>Step 20</td>
<td><strong>exit</strong></td>
<td>Ends the controller session and returns to the configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Router(config-controller)# exit</em></td>
<td></td>
</tr>
<tr>
<td>Step 21</td>
<td><strong>interface</strong> <strong>POS</strong> <em>slot/bay/port</em></td>
<td>Configures a serial interface and enters the interface configuration mode</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Router(config)# interface POS 0/5/2</em></td>
<td></td>
</tr>
<tr>
<td>Step 22</td>
<td><strong>ip address</strong> <strong>ip-address</strong></td>
<td>Assigns the ip address to POS interface</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Router(config-if)# ip address 45.1.1.2 255.255.255.0</em></td>
<td></td>
</tr>
<tr>
<td>Step 23</td>
<td><strong>encapsulation</strong> <strong>ppp</strong></td>
<td>Specifies the ppp encapsulation over POS interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Router(config-if-srv)# encapsulation ppp</em></td>
<td></td>
</tr>
<tr>
<td>Step 24</td>
<td><strong>end</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Router(config-if-srv)# end</em></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring protect node for POS MR-APS

To configure MR-APS protect node for POS interface, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. exit
4. redundancy
5. interchassis group group-id
6. member ip ip-address
7. monitor peer bfd
8. exit
9. controller SONET slot/bay/port
10. framing [SDH | SONET]
11. clock source internal
12. sts-1 1-3POS
13. exit
14. controller SONET slot/bay/port
15. Shutdown
16. aps group group_id
17. aps protect 1 remote loopback ip
18. aps interchasis group interchasis group-id
19. no shut
20. exit
21. interface POS slot/bay/port
22. ip address ip-address
23. encapsulation ppp
24. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</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&gt; 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>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>exit</td>
<td>Exits PW class configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-pw-class)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>redundancy</td>
<td>Enters the redundancy configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# redundancy</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures an interchassis group within the redundancy configuration mode and enters the interchassis redundancy mode.</td>
<td></td>
</tr>
<tr>
<td><strong>interchassis group</strong> <em>group-id</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-red)# <strong>interchassis group</strong> 50</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Configures the IP address of the peer member group.</td>
<td></td>
</tr>
<tr>
<td><strong>member ip</strong> <em>ip-address</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-r-ic)# <strong>member ip</strong> 60.60.60.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Enables BFD on the POS link.</td>
<td></td>
</tr>
<tr>
<td><strong>monitor peer bfd</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-red)# <strong>monitor peer bfd</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Exits the redundancy mode.</td>
<td></td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-r-ic)# <strong>exit</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Selects and configures a SONET controller and enters controller configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>controller SONET</strong> <em>slot/bay/port</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config)# <strong>controller SONET</strong> 0/5/2</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Configures the controller with framing type. SONET framing is the default option.</td>
<td></td>
</tr>
<tr>
<td>**framing [SDH</td>
<td>SONET]**</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# <strong>framing SONET</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Sets the clocking for individual E1 links.</td>
<td></td>
</tr>
<tr>
<td><strong>clock source internal</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# <strong>clock source internal</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Specifies the STS identifier.</td>
<td></td>
</tr>
<tr>
<td><strong>sts-l 1-3POS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# <strong>sts-l 1-3</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>Exits from the STS configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-ctrlr-sts1)# <strong>exit</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>Selects and configures a SONET controller and enters controller configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>controller SONET</strong> <em>slot/bay/port</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config)# <strong>controller SONET</strong> 0/5/2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>15</td>
<td><strong>Shutdown</strong></td>
<td>Shut down the controller before APS configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# <strong>Shutdown</strong></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td><strong>aps group</strong> <em>group_id</em></td>
<td>Configures the APS group for POS.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# <strong>aps group 1</strong></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td><strong>aps protect 1</strong> <em>remote loopback ip</em></td>
<td>Enable the protect node.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# <strong>aps protect 1</strong> 192.168.1.1</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td><strong>aps interchasis group</strong> <em>interchasis group-id</em></td>
<td>Enable the inter chasis.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# <strong>aps interchasis group 1</strong></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td><strong>no shut</strong></td>
<td>Unshut the controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# <strong>no shut</strong></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td><strong>exit</strong></td>
<td>Ends the controller session and returns to the configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# <strong>exit</strong></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td><strong>interface POS</strong> <em>slot/bay/port</em></td>
<td>Configures a serial interface and enters the interface configuration mode</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# <strong>interface POS 0/5/2</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>slot</strong>—Chassis slot number, which is always 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>bay</strong>—Card interface bay number in a slot. The range is from 0 to 5.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>port</strong>—Port or interface number. The range can be 0-3.</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td><strong>ip address</strong> <em>ip-address</em></td>
<td>Assigns the ip address to POS interface</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# <strong>ip address 45.1.1.2 255.255.255.0</strong></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td><strong>encapsulation ppp</strong></td>
<td>Specifies the ppp encapsulation over POS interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# <strong>encapsulation ppp</strong></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td><strong>end</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Verifying MR-APS on POS interface

- Use the `show rgf groups` command to display POS statistics for the configured POS circuits.

Following is a sample output of the `show rgf groups` command to display the detailed information about POS interface configured on the router:

```
Router# show rgf groups

Router# sh rgf groups
Total RGF groups: 2
----------------------------------------------------------
ACTIVE RGF GROUP
  RGF Group ID : 1
  RGF Peer Group ID: 0
  ICRM Group ID : 1
  APS Group ID : 1

RGF State information:
  My State Present : Active-fast <<<<<<<<<<Chk this status
  Previous : Standby-hot
  Peer State Present: Standby-hot
  Previous: Standby-bulk

Misc:
  Communication state Up
  apsBulk: 0
  apsStby: 0
  peerStby: 0
  -> Driven Peer to [Peer Standby Hot] Progression
  -> Standby sent Bulk Sync start Progression
  RGF GET BUF: 66  RGF RET BUF 66
```

Following is a sample output of the `show ppp interface POS`

```
Router# show ppp interface 0/5/2

PPP Serial Context Info
--------------------
  Interface : PO0/4/2.1
  PPP Serial Handle: 0xE9000006
  PPP Handle : 0xBF000006
  SSS Handle : 0x8000006
  AAA ID : 14
  Access IE : 0xA000006
  SHDB Handle : 0xA3000006
  State : Up
  Last State : Binding
  Last Event : LocalTerm
```

- Use the `show ccm group id group-id number` command to check CCM status

```
Router# show ccm group id
```
CCM Group 1 Details
----------------------------------------
CCM Group ID : 1
Infra Group ID : 2
Infra Type : Redundancy Group Facility (RGF) <<<<Chk this
HA State : CCM HA Active
Redundancy State : Dynamic Sync
Group Initialized/cleaned : FASLE

• Following is a sample output of the show aps gr 1 command:

```
Router# show aps gr 1
SONET 0/4/2 APS Group 1: working channel 1 (Inactive) (HA)
 Protect at 33.1.1.1
 PGP timers (from protect): hello time=1; hold time=10
 SDH framing
 Remote APS configuration: (null)
```

• Following is a sample output of the show redundancy interchassis command to display information about interchassis redundancy group configuration:

```
Router# show redundancy interchassis
Redundancy Group 1 (0x1)
 Applications connected: MSR
 Monitor mode: BFD
 member ip: 10.17.255.163 "ASR903 PE2", CONNECTED
          BFD neighbor: GigabitEthernet0/1/2, next hop 33.1.1.2, DOWN
          MSR state: CONNECTED

ICRM fast-failure detection neighbor table
 IP Address Status Type Next-hop IP Interface
 ========== ======= ======== =========
 10.17.255.163 DOWN BFD 33.1.1.2 GigabitEthernet0/1/2
```

Configuration Examples for MR-APS on POS interface

The following example shows how to configure the MR-APS integration on a POS interface on the working router PE1 working node:

```
RouterPE1> enable
RouterPE1(config)#cont so 0/4/2
RouterPE1(config-controller)#au-4 1 pos
RouterPE1(config-controller)#aps gr 1
RouterPE1(config-controller)#aps working 1
RouterPE1(config-controller)#aps interchassis group 1
RouterPE1(config-controller)#exit
RouterPE1(config)#interface POS0/4/2.1
RouterPE1(config-if)#ip address 45.1.1.2
RouterPE1(config-if)#encapsulation ppp
RouterPE1(config)# redundancy
RouterPE1(config-red)# interchassis group 1
RouterPE1(config-red-ic)# member ip 14.2.0.2
RouterPE1(config-red-ic)# backbone interface gig 0/0/1
```
The following example shows how to configure the MR-APS integration on a POS interface on the Protect router PE2 Protect node:

RouterPE2> enable  
RouterPE2(config)#cont so 0/4/2  
RouterPE2(config-controller)#framing sdh  
RouterPE2(config-controller)#clock source line  
RouterPE2(config-controller)#aug mapping au-4  
RouterPE2(config-controller)#au-4 1 pos  
RouterPE2(config-controller)#aps group 1  
RouterPE2(config-controller)#aps protect 1 1.1.1.1  
RouterPE2(config-controller)#aps interchassis group 1  
RouterPE1(config-controller)#exit  
RouterPE2(config)#interface POS0/4/2.1  
RouterPE2(config-interface)#ip address 45.1.1.1 255.255.255.0  
RouterPE2(config-interface)#encapsulation ppp  
RouterPE2(config-controller)#network-clock input-source 1 controller SONET 0/4/2  
RouterPE2(config)# redundancy  
RouterPE2(config)#mode sso  
RouterPE2(config-red)#interchassis group 1  
RouterPE2(config-r-ic)#monitor peer bfd  
RouterPE2(config-r-ic)#member ip 52.1.1.1  
RouterPE2(config-r-ic)# exit

The following example shows how to configure the MR-APS integration on a POS interface on the router CE1 working node:

RouterPE3> enable  
RouterPE3(config)#cont SONET 0/3/1  
RouterPE3(config-controller)#framing sdh  
RouterPE3(config-controller)#clock source line  
RouterPE3(config-controller)#aug mapping au-4  
RouterPE3(config-controller)#au-4 1 pos  
RouterPE3(config)#interface POS0/4/2.1  
RouterPE3(config-interface)#ip address 45.1.1.1 255.255.255.0  
RouterPE3(config-interface)#encapsulation ppp  
RouterPE3(config-controller)#network-clock input-source 1 controller SONET 0/4/2  
RouterPE3(config-controller)#exit
Hot Standby Pseudowire Support for ATM and TDM Access Circuits

Note

Hot Standby Pseudowire Support for ATM and IMA circuits are not supported on the Cisco ASR 900 RSP3 module.

The Hot Standby Pseudowire Support for ATM and TDM Access Circuits feature is an enhancement to the L2VPN Pseudowire Redundancy feature in the following ways:

• Faster failover of to the backup pseudowire
• Less traffic loss during failover

The Hot Standby Pseudowire Support for ATM and TDM Access Circuits feature allows the backup pseudowire to be in a “hot standby” state, so that it can immediately take over if the primary pseudowire fails. The following sections explain the concepts and configuration tasks for this feature.

• Finding Feature Information, on page 85
• Prerequisites for Hot Standby Pseudowire Support for ATM and TDM Access Circuits, on page 86
• Restrictions for Hot Standby Pseudowire Support for ATM and TDM Access Circuits, on page 86
• Information About Hot Standby Pseudowire Support for ATM and TDM Access Circuits, on page 86
• How to Configure Hot Standby Pseudowire Support for ATM and TDM Access Circuits, on page 87
• Configuration Examples for Hot Standby Pseudowire Support for ATM and TDM Access Circuits, on page 93
• Additional References, on page 94

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Prerequisites for Hot Standby Pseudowire Support for ATM and TDM Access Circuits

- This feature requires that you understand how to configure Layer 2 virtual private networks (VPNs). You can find that information in the following documents:
  - Any Transport over MPLS
  - L2 VPN Interworking
  - L2VPN Pseudowire Redundancy

- The Hot Standby Pseudowire Support for ATM and TDM Access Circuits feature recommends that the following mechanisms be in place to enable faster detection of a failure in the network:
  - Label-switched paths (LSP) Ping/Traceroute and Any Transport over MPLS Virtual Circuit Connection Verification (AToM VCCV)
  - Local Management Interface (LMI)
  - Operation, Administration, and Maintenance (OAM)

Restrictions for Hot Standby Pseudowire Support for ATM and TDM Access Circuits

- Hot Standby Pseudowire Support for ATM and TDM Access Circuits is not supported on L2TPv3. Only MPLS L2VPNs are supported.
- Hot Standby Pseudowire Support for ATM and IMA is not supported on the Cisco ASR 900 RSP3 module.
- More than one backup pseudowire is not supported.
- Different pseudowire encapsulation types on the MPLS pseudowire are not supported.
- If you use Hot Standby Pseudowire Support for ATM and TDM Access Circuits with L2VPN Interworking, the interworking method must be the same for the primary and backup pseudowires. For TDM access circuits, interworking is not supported.
- Only dynamic pseudowires are supported.
- Pseudowire over static VPLS is not supported on the Cisco ASR 900 RSP3 module.
Information About Hot Standby Pseudowire Support for ATM and TDM Access Circuits

How the Hot Standby Pseudowire Support for ATM and TDM Access Circuits Feature Works

The Hot Standby Pseudowire Support for ATM and TDM Access Circuits feature improves the availability of L2VPN pseudowires by detecting failures and handling them with minimal disruption to the service.

The Hot Standby Pseudowire Support for ATM and TDM Access Circuits feature allows the backup pseudowire to be in a “hot standby” state, so that it can immediately take over if the primary pseudowire fails. The L2VPN Pseudowire Redundancy feature allows you to configure a backup pseudowire too, but in a cold state. With the L2VPN Pseudowire Redundancy feature, if the primary pseudowire fails, it takes time for the backup pseudowire to take over, which causes a loss in traffic.

If you have configured L2VPN Pseudowire Redundancy on your network and upgrade to Cisco IOS Release 15.1(1)S, you do not need add any other commands to achieve Hot Standby Pseudowire Support for ATM and TDM Access Circuits. The backup pseudowire will automatically be in a hot standby state.

Supported Transport Types

The Hot Standby Pseudowire Support for ATM and TDM Access Circuits feature supports the following transport types:

- ATM
  - ATM AAL5 in VC mode
  - ATM packed cell relay in VC Mode
  - ATM in VP mode
  - ATM packed cell relay in VP mode
  - ATM in port mode
  - ATM packed cell relay in port mode
- Time division multiplexing (TDM)
  - Structure-Agnostic TDM over Packet (SAToP)
  - Circuit Emulation Services over PSN (CESoPSN)

How to Configure Hot Standby Pseudowire Support for ATM and TDM Access Circuits

The Hot Standby Pseudowire Support for ATM and TDM Access Circuits feature enables you to configure a backup pseudowire in case the primary pseudowire fails. When the primary pseudowire fails, the PE router can immediately switch to the backup pseudowire.
Configuring a Pseudowire for Static VPLS

Pseudowire for Static VPLS is *not* supported on the Cisco ASR 900 RSP3 module.

The configuration of pseudowires between provider edge (PE) devices helps in the successful transmission of the Layer 2 frames between PE devices.

Use the pseudowire template to configure the virtual circuit (VC) type for the virtual path identifier (VPI) pseudowire. In the following task, the pseudowire will go through a Multiprotocol Label Switching (MPLS)-Tunneling Protocol (TP) tunnel.

The pseudowire template configuration specifies the characteristics of the tunneling mechanism that is used by the pseudowires, which are:

- Encapsulation type
- Control protocol
- Payload-specific options
- Preferred path

Perform this task to configure a pseudowire template for static Virtual Private LAN Services (VPLS).

Ensure that you perform this task before configuring the virtual forwarding instance (VFI) peer. If the VFI peer is configured before the pseudowire class, the configuration is incomplete until the pseudowire class is configured. The `show running-config` command displays an error stating that configuration is incomplete.

```
Device# show running-config | sec vfi
l2 vfi config manual
vpn id 1000
! Incomplete point-to-multipoint vfi config
```

**SUMMARY STEPS**

1. enable
2. configure terminal
3. template type pseudowire *name*
4. encapsulation mpls
5. signaling protocol none
6. preferred-path interface Tunnel-tp *interface-number*
7. exit
8. interface pseudowire *number*
9. source template type pseudowire *name*
10. neighbor *peer-address* *vcid-value*
11. label local-pseudowire-label remote-pseudowire-label
12. end
## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</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></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></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></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the template type as pseudowire and enters template configuration mode.</td>
</tr>
<tr>
<td>template type pseudowire <em>name</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# template type pseudowire static-vpls</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies the tunneling encapsulation.</td>
</tr>
<tr>
<td>encapsulation mpls</td>
<td>• For Any Transport over MPLS (AToM), the encapsulation type is MPLS.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-template)# encapsulation mpls</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies that no signaling protocol is configured for the pseudowire class.</td>
</tr>
<tr>
<td>signaling protocol none</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-template)# signaling protocol none</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Specifies the path that traffic uses: an MPLS Traffic Engineering (TE) tunnel or destination IP address and Domain Name Server (DNS) name.</td>
</tr>
<tr>
<td>preferred-path interface Tunnel-tp <em>interface-number</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-template)# preferred-path interface Tunnel-tp 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Exits template configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-template)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Establishes a pseudowire interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>interface pseudowire <em>number</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface pseudowire 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Configures the source template type of the configured pseudowire.</td>
</tr>
<tr>
<td>source template type pseudowire <em>name</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# source template type pseudowire name</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Hot Standby Pseudowire Support for ATM and TDM Access Circuits

Use the following steps to configure the Hot Standby Pseudowire Support for ATM and TDM Access Circuits feature.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface atm number`
4. `pvc [name] vpi/vci l2transport`
5. `xconnect peer-router-id vcid [encapsulation mpls] pw-class pw-class-name`
6. `backup peer peer-router-ip-addr vcid [pw-class pw-class-name]`
7. `backup delay enable-delay {disable-delay | never}`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | Enables privileged EXEC mode.  
* Enter your password if prompted. |
| `enable` | Enters global configuration mode. |
| **Example:**  
Router> enable | |
| **Step 2** | |
| `configure terminal` | |
| **Example:**  
Router# configure terminal | |
## Purpose

Command or Action | Purpose |
--- | --- |
**Step 3** | Specifies the ATM interface and enters interface configuration mode. |
*interface atm number*  
*Example:*  
Router(config)# interface atm4/1/0 | |
**Step 4** | Creates or assigns a name to an ATM PVC and enters L2transport PVC configuration mode. |
*pvc [name] vpi/vci l2transport*  
*Example:*  
Router(config-if)# pvc 1/100 l2transport | |
**Step 5** | Binds the attachment circuit to a pseudowire VC. |
*xconnect peer-router-id vcid {encapsulation mpls}  
   pw-class pw-class-name*  
*Example:*  
Router(config-if-atm-l2trans-pvc)# xconnect 10.0.0.1 123 pw-class atom | |
**Step 6** | Specifies a redundant peer for the pseudowire VC.  
The pseudowire class name must match the name you specified when you created the pseudowire class, but you can use a different pw-class in the *backup peer* command than the name that you used in the primary *xconnect* command. |
*backup peer peer-router-ip-addr vcid [pw-class pw-class-name]*  
*Example:*  
Router(config-if-atm-l2trans-pvc)# backup peer 10.0.0.3 125 pw-class atom | |
**Step 7** | Specifies how long (in seconds) the backup pseudowire VC should wait to take over after the primary pseudowire VC goes down. The range is 0 to 180.  
Specifies how long the primary pseudowire should wait after it becomes active to take over for the backup pseudowire VC. The range is 0 to 180 seconds. If you specify the *never keyword*, the primary pseudowire VC never takes over for the backup. |
*backup delay enable-delay {disable-delay | never}*  
*Example:*  
Router(config-if-atm-l2trans-pvc)# backup delay 5 never | |

## Verifying the Hot Standby Pseudowire Support for ATM and TDM Access Circuits Configuration

Use the following commands to verify that the backup pseudowire is provisioned for hot standby support.

**SUMMARY STEPS**

1. *show atm acircuit*
2. *show atm pvc*
3. *show cem acircuit*
4. *show cem acircuit detail*
DETAILED STEPS

Step 1  
**show atm acircuit**

If the output of the `show atm acircuit` command shows two entries for the same vpi/vci, then the backup pseudowire has been correctly provisioned, as shown in the following example:

**Example:**

```
Router# show atm acircuit

Interface  VPI  VCI  AC Id  Switch  Segment  St  Flg  Prov
----------  ---  ---  --  --  -------  -------  --  ---  ----
ATM2/1/0.2  11  111  ATA5  1  2003    4007    2  0  Y
ATM2/1/0.2  11  111  ATA5  1  1002    3006    2  0  Y
```

Step 2  
**show atm pvc**

If the output of the `show atm pvc` command includes “Red Prov: Yes,” then the backup pseudowire has been correctly provisioned, as shown in bold in the following example:

**Example:**

```
Router# show atm pvc 1/1010

Interworking Method: like to like
AC Type: ATM AAL5, Circuit Id: 2, AC State: UP, Prov: YES
Switch Hdl: 0x1005, Segment hdl: 0x4011
Red Switch Hdl: 0x3007, Red Segment hdl: 0x6010, Red Prov: YES
AC Hdl: 0x7200000F, AC Peer Hdl: 0x5D000012, Flg:0, Platform Idx:10
Status: UP
```

Step 3  
**show cem acircuit**

If the output of the `show cem acircuit` command includes “Redundancy Member Prov: Yes,” then the backup pseudowire has been correctly provisioned, as shown in bold in the following example:

**Example:**

```
Router# show cem acircuit

CEM Int.  ID  Flags  Swhdl  Seghdl  Ckt_type  Provisioned
---------  --  ----  ------  -------  --------  ----------------
CEM3/0/0   1  0     B00E    201E     19        Yes
Redundancy Switch hdl: 0xC00F Redundancy Segment hdl: 0x401F
Redundancy Member Prov: Yes
```

Step 4  
**show cem acircuit detail**

If the output of the `show cem acircuit detail` command includes “Redundancy Member Prov: Yes,” then the backup pseudowire has been correctly provisioned, as shown in bold in the following example:

**Example:**

```
Router# show cem acircuit detail

CEM3/0/0  Cemid 1
PW Ckt_Type: 19  Aie hdl: EE00000B Peer aie hdl: 0x2000000C
Switch hdl: 0x800E  Segment hdl: 0x201E  Redundancy Switch hdl: 0x1000
Redundancy Segment hdl: 0x4002  Redundancy Member Prov: Yes
```
Configuration Examples for Hot Standby Pseudowire Support for ATM and TDM Access Circuits

Configuring Hot Standby Pseudowire Support for ATM and TDM Access Circuits on CEM Circuits Example

The figure below shows the configuration of Hot Standby Pseudowire Support for ATM and TDM Access Circuits, where the backup pseudowire is on the same PE router.

Figure 9: Hot Standby Pseudowire Topology

The configuration shown in the figure above is used in the following examples:

Table 4: Configuring Hot Standby Pseudowire Support for ATM and TDM Access Circuits on CEM Circuits: Example

<table>
<thead>
<tr>
<th>PE1</th>
<th>PE2</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface Loopback0</td>
<td>interface Loopback0</td>
</tr>
<tr>
<td>ip address 10.4.4.4 255.255.255.255</td>
<td>ip address 10.2.2.2 255.255.255.255</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>Controller E1 9/2/0</td>
<td>Controller E1 2/2/0</td>
</tr>
<tr>
<td>clock source internal</td>
<td>clock source internal</td>
</tr>
<tr>
<td>cem-group 0 timeslots 1-4</td>
<td>cem-group 0 timeslots 1-4</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>pseudowire-class atom</td>
<td>pseudowire-class atom</td>
</tr>
<tr>
<td>encapsulation mpls</td>
<td>encapsulation mpls</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface CEM9/2/0</td>
<td>interface CEM2/2/0</td>
</tr>
<tr>
<td>no ip address</td>
<td>no ip address</td>
</tr>
<tr>
<td>class int cesopsn_1</td>
<td>class int cesopsn_1</td>
</tr>
<tr>
<td>cem 0</td>
<td>cem 0</td>
</tr>
<tr>
<td>xconnect 10.2.2.2 5000 pw-class atom</td>
<td>xconnect 10.2.2.2 5000 pw-class atom</td>
</tr>
<tr>
<td>backup peer 10.2.2.2 5005 pw-class atom</td>
<td>backup peer 10.2.2.2 5005 pw-class atom</td>
</tr>
<tr>
<td>backup delay 0 5</td>
<td>backup delay 0 5</td>
</tr>
<tr>
<td></td>
<td>xconnect 10.4.4.4 5000 encapsulation mpls</td>
</tr>
<tr>
<td></td>
<td>xconnect 10.4.4.4 5000 encapsulation mpls</td>
</tr>
</tbody>
</table>
Table 5: Configuring Hot Standby Pseudowire Support for ATM and TDM Access Circuits on ATM Circuits: Example

<table>
<thead>
<tr>
<th>PE1</th>
<th>PE2</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface Loopback0</td>
<td>interface Loopback0</td>
</tr>
<tr>
<td>ip address 10.44.44.4 255.255.255.255</td>
<td>ip address 10.22.22.22 255.255.255.255</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface POS3/3/0</td>
<td>interface POS3/3/0</td>
</tr>
<tr>
<td>ip address 10.4.4.4 255.255.255.0</td>
<td>ip address 10.4.4.1 255.255.255.0</td>
</tr>
<tr>
<td>mpls ip</td>
<td>mpls ip</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface ATM4/1/0</td>
<td>interface ATM4/1/0</td>
</tr>
<tr>
<td>no ip address</td>
<td>no ip address</td>
</tr>
<tr>
<td>no atm enable-ilm-trap</td>
<td>no atm enable-ilm-trap</td>
</tr>
<tr>
<td>pvc 1/100 l2transport</td>
<td>pvc 1/100 l2transport</td>
</tr>
<tr>
<td>xconnect 10.22.22.22 1 encapsulation mpls</td>
<td>xconnect 10.44.44.4 1 encapsulation mpls</td>
</tr>
<tr>
<td>backup peer 10.22.22.22 2</td>
<td>backup peer 10.44.44.4 2</td>
</tr>
</tbody>
</table>

Additional References

The following sections provide references related to the Hot Standby Pseudowire Support for ATM and TDM Access Circuits feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td><em>Cisco IOS Master Commands List, All Releases</em></td>
</tr>
<tr>
<td>MPLS commands</td>
<td><em>Cisco IOS Multiprotocol Label Switching Command Reference</em></td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-muley-pwe3-redundancy</td>
<td>Pseudowire Redundancy</td>
</tr>
<tr>
<td>draft-ietf-pwe3-iccp-xx.txt</td>
<td>Inter-Chassis Communication Protocol for L2VPN PE Redundancy</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-IETF-PW-ATM-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 5085</td>
<td>Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
CHAPTER 5

PPP and Multilink PPP Configuration

Note

PPP and Multilink PPP Configuration is not supported on the Cisco ASR 900 RSP3 module.

This module describes how to configure PPP and Multilink PPP (MLP) features on any interface. Multilink PPP provides a method for spreading traffic across multiple physical WAN links.

- Limitations, on page 97
- PPP and Multilink PPP, on page 98
- IP Address Pooling, on page 99
- How to Configure PPP, on page 101
- Monitoring and Maintaining PPP and MLP Interfaces, on page 122

Limitations

The following limitations apply when using MLPPP on the Cisco ASR 903 Router:

- All links in an MLPPP bundle must be on the same interface module.
- All links in an MLPPP bundle must be of the same bandwidth.
- The router supports a maximum of 16 links per bundle and a minimum of 2 links per bundle. Maximum number of bundles supported per interface module is 168.
- To change the MLPPP bundle fragmentation mode between enabled and disabled, perform a `shutdown/no shutdown` on the bundle.
- LFI is not supported. However, PPP Multilink fragmentation is supported by default. To disable fragmentation, see Disabling PPP Multilink Fragmentation.
- Multicast MLP is not supported.
- PPP compression is not supported.
- PPP half bridging is not supported.
- IPv6 is not supported for this feature.
- To enable an ACFC or PFC configuration, issue a shut `shutdown/no shutdown` on the serial interface.
• Channelization is not supported
• Also that only 1 channel-group can be created per controller with complete timeslots.
• PPP and MLPPP are supported on synchronous serial interfaces; Asynchronous serial interfaces, high-speed serial interfaces (HSSI), and ISDN interfaces are not supported.
• If you configure interfaces on each end of an MLPPP connection with different MTU values, the link drops traffic at high traffic rates. We recommend that you configure the same MTU values across all nodes in an MLPPP connection.

PPP and Multilink PPP

To configure the Media-Independent PPP and Multilink PPP, you should understand the following concepts:

Point-to-Point Protocol

Point-to-Point Protocol (PPP), described in RFC 1661, encapsulates network layer protocol information over point-to-point links. You can configure PPP on synchronous serial interfaces. Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), or Password Authentication Protocol (PAP)

Magic Number support is available on all serial interfaces. PPP always attempts to negotiate for Magic Numbers, which are used to detect looped-back lines. Depending on how the down-when-looped command is configured, the router might shut down a link if it detects a loop.

CHAP or PPP Authentication

PPP with CHAP or PAP authentication is often used to inform the central site about which remote routers are connected to it.

With this authentication information, if the router or access server receives another packet for a destination to which it is already connected, it does not place an additional call. However, if the router or access server is using rotaries, it sends the packet out the correct port.

CHAP and PAP were originally specified in RFC 1334, and CHAP was updated in RFC 1994. These protocols are supported on synchronous and asynchronous serial interfaces. When using CHAP or PAP authentication, each router or access server identifies itself by a name. This identification process prevents a router from placing another call to a router to which it is already connected, and also prevents unauthorized access.

Access control using CHAP or PAP is available on all serial interfaces that use PPP encapsulation. The authentication feature reduces the risk of security violations on your router or access server. You can configure either CHAP or PAP for the interface.

Note

To use CHAP or PAP, you must be running PPP encapsulation.

When CHAP is enabled on an interface and a remote device attempts to connect to it, the local router or access server sends a CHAP packet to the remote device. The CHAP packet requests or “challenges” the remote
device to respond. The challenge packet consists of an ID, a random number, and the hostname of the local router.

The required response has two parts:

- An encrypted version of the ID, a secret password, and the random number
- Either the hostname of the remote device or the name of the user on the remote device

When the local router or access server receives the response, it verifies the secret password by performing the same encryption operation as indicated in the response and looking up the required hostname or username. The secret passwords must be identical on the remote device and the local router.

Because this response is sent, the password is never sent in clear text, preventing other devices from stealing it and gaining illegal access to the system. Without the proper response, the remote device cannot connect to the local router.

CHAP transactions occur only when a link is established. The local router or access server does not request a password during the rest of the call. (The local device can, however, respond to such requests from other devices during a call.)

When PAP is enabled, the remote router attempting to connect to the local router or access server is required to send an authentication request. The username and password specified in the authentication request are accepted, and the Cisco IOS software sends an authentication acknowledgment.

After you have enabled CHAP or PAP, the local router or access server requires authentication from remote devices. If the remote device does not support the enabled protocol, no traffic will be passed to that device.

To use CHAP or PAP, you must perform the following tasks:

- Enable PPP encapsulation.
- Enable CHAP or PAP on the interface.

For CHAP, configure hostname authentication and the secret password for each remote system with which authentication is required.

**IP Address Pooling**

A point-to-point interface must be able to provide a remote node with its IP address through the IP Control Protocol (IPCP) address negotiation process. The IP address can be obtained from a variety of sources. The address can be configured through the command line, entered with an EXEC-level command, provided by TACACS+ or the Dynamic Host Configuration Protocol (DHCP), or from a locally administered pool.

IP address pooling uses a pool of IP addresses from which an incoming interface can provide an IP address to a remote node through IPCP address negotiation process. IP address pooling also enhances configuration flexibility by allowing multiple types of pooling to be active simultaneously.

The IP address pooling feature allows configuration of a global default address pooling mechanism, per-interface configuration of the address pooling mechanism, and per-interface configuration of a specific address or pool name.

**Peer Address Allocation**

A peer IP address can be allocated to an interface through several methods:
Precedence Rules

The following precedence rules of peer IP address support determine which address is used. Precedence is listed from most likely to least likely:

1. AAA/TACACS+ provided address or addresses from the pool named by AAA/TACACS+
2. An address from a local IP address pool or DHCP (typically not allocated unless no other address exists)
3. Dialer map lookup address (not done unless no other address exists)
4. Address from an EXEC-level PPP command, or from a chat script
5. Configured address from the peer default ip address command or address from the protocol translate command
6. Peer-provided address from IPCP negotiation (not accepted unless no other address exists)
MLP on Synchronous Serial Interfaces

Address pooling is available on all synchronous serial interfaces that are running PPP and PPPoX sessions. MLP provides characteristics are most similar to hardware inverse multiplexers, with good manageability and Layer 3 services support. Figure below shows a typical inverse multiplexing application using two Cisco routers and Multilink PPP over four T1 lines.

How to Configure PPP

The sections below describe how to configure PPP.

Enabling PPP Encapsulation

The `encapsulation ppp` command enables PPP on serial lines to encapsulate IP and other network protocol datagrams.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. `interface serial slot/subslot/port:channel`
4. `encapsulation ppp`
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><code>interface serial slot/subslot/port:channel</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# interface serial 0/0/0:0</code></td>
<td></td>
</tr>
</tbody>
</table>
Enabling CHAP or PAP Authentication

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface serial number`
4. `ppp authentication {chap | chap pap | pap chap | pap} [if-needed] [list-name | default] [callin]`
5. `ppp use-tacacs [single-line] or aaa authentication ppp`
6. `exit`
7. `username name [user-maxlinks link-number] password secret`
8. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
| Example:          | • Enter your password if prompted. |
|                   | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example:          | Router# configure terminal |
| **Step 3** interface serial number | Enters Interface Configuration mode. |
| Example:          | Router(config)# interface serial 0/0/0 |
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>`ppp authentication {chap</td>
<td>chap pap</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Router(config-if)# ppp authentication chap</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>:</td>
<td>- Use the <code>ppp authentication chap</code> command only with TACACS or extended TACACS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- With AAA configured on the router and list names defined for AAA, the <code>list-name</code> optional argument can be used with AAA/TACACS+. Use the <code>ppp use-tacacs</code> command with TACACS and Extended TACACS. Use the <code>aaa authentication ppp</code> command with AAA/TACACS+.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>ppp use-tacacs [single-line]</code> or <code>aaa authentication ppp</code></td>
<td>Configure TACACS on a specific interface as an alternative to global host authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Router(config-if)# ppp use-tacacs single-line</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# aaa authentication ppp</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>exit</code></td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Router(config-if)# exit</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>username name [user-maxlinks link-number] password secret</code></td>
<td>Configures identification.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Router(config)# username name user-maxlinks 1 password password1</code></td>
<td>- Optionally, you can specify the maximum number of connections a user can establish.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To use the <code>user-maxlinks</code> keyword, you must also use the <code>aaa authorization network default local</code> command and PPP encapsulation and name authentication on all the interfaces the user will be accessing.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>end</code></td>
<td>Exits global configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Router(config)# end</code></td>
<td><strong>Caution</strong>: If you use a list name that has not been configured with the <code>aaa authentication ppp</code> command, you disable PPP on the line.</td>
</tr>
</tbody>
</table>

**Example**

```
Router# configure terminal
Router(config)# interface serial 0/0/0
```
Configuring IP Address Pooling

You can define the type of IP address pooling mechanism used on router interfaces in one or both of the ways described in the following sections:

---

**Note**

For more information about address pooling, see the IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S

---

Global Default Address Pooling Mechanism

The global default mechanism applies to all point-to-point interfaces that support PPP encapsulation and that have not otherwise been configured for IP address pooling. You can define the global default mechanism to be either DHCP or local address pooling.

To configure the global default mechanism for IP address pooling, perform the tasks in the following sections:

- Defining DHCP as the Global Default Mechanism
- Defining Local Address Pooling as the Global Default Mechanism

After you have defined a global default mechanism, you can disable it on a specific interface by configuring the interface for some other pooling mechanism. You can define a local pool other than the default pool for the interface or you can configure the interface with a specific IP address to be used for dial-in peers.

You can also control the DHCP network discovery mechanism; see the following section for more information:

- Controlling DHCP Network Discovery

Defining DHCP as the Global Default Mechanism

DHCP specifies the following components:

- A DHCP server—A host-based DHCP server configured to accept and process requests for temporary IP addresses.
- A DHCP proxy client—A Cisco access server configured to arbitrate DHCP calls between the DHCP server and the DHCP client. The DHCP client-proxy feature manages a pool of IP addresses available to dial-in clients without a known IP address.

Perform this task to enable DHCP as the global default mechanism.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip address-pool dhcp-proxy-client
4. `ip dhcp-server [ip-address | name]`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</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**
| `ip address-pool dhcp-proxy-client`
| Example: `Router(config)# ip address-pool dhcp-proxy-client`
| Specifies the DHCP client-proxy feature as the global default mechanism.  
- The `peer default ip address` command and the `member peer default ip address` command can be used to define default peer IP addresses.
| **Note** You can provide as few as one or as many as ten DHCP servers for the proxy client (the Cisco router or access server) to use. The DHCP servers provide temporary IP addresses. |
| **Step 4**
| `ip dhcp-server [ip-address | name]`
| Example: `Router(config)# ip dhcp-server 209.165.201.1`
| (Optional) Specifies the IP address of a DHCP server for the proxy client to use. |
| **Step 5**
| `end`
| Example: `Router(config)# end`
|Exits global configuration mode. |

**Defining Local Address Pooling as the Global Default Mechanism**

Perform this task to define local address pooling as the global default mechanism.

*Note* If no other pool is defined, a local pool called “default” is used. Optionally, you can associate an address pool with a named pool group.
SUMMARY STEPS

1. enable
2. configure terminal
3. ip address-pool local
4. ip local pool {named-address-pool | default} first-IP-address [last-IP-address] [group group-name] [cache-size size]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
<td>Example: Router&gt; enable</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
<td>Example: Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 ip address-pool local</td>
<td>Specifies local address pooling as the global default mechanism.</td>
<td>Example: Router(config)# ip address-pool local</td>
</tr>
<tr>
<td>Step 4 ip local pool {named-address-pool</td>
<td>default} first-IP-address [last-IP-address] [group group-name] [cache-size size]</td>
<td>Creates one or more local IP address pools.</td>
</tr>
</tbody>
</table>

Controlling DHCP Network Discovery

Perform the steps in this section to allow peer routers to dynamically discover Domain Name System (DNS) and NetBIOS name server information configured on a DHCP server using PPP IPCP extensions.

The ip dhcp-client network-discovery global configuration command provides a way to control the DHCP network discovery mechanism. The number of DHCP Inform or Discovery messages can be set to 1 or 2, which determines how many times the system sends the DHCP Inform or Discover messages before stopping network discovery. You can set a timeout period from 3 to 15 seconds, or leave the default timeout period at 15 seconds. The default for the informs and discovers keywords is 0, which disables the transmission of these messages.

Note For more information about DHCP, see the IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S.
**SUMMARY STEPS**

1. enable
2. configure terminal
3. `ip dhcp-client network-discovery informs number-of-messages discovers number-of-messages period seconds`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Provides control of the DHCP network discovery mechanism by allowing the number of DHCP Inform and Discover messages to be sent, and a timeout period for retransmission, to be configured.</td>
</tr>
<tr>
<td><code>ip dhcp-client network-discovery informs number-of-messages discovers number-of-messages period seconds</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# ip dhcp-client network-discovery informs 2 discovers 2 period 2</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring IP Address Assignment**

Perform this task to configure IP address alignment.

After you have defined a global default mechanism for assigning IP addresses to dial-in peers, you can configure the few interfaces for which it is important to have a nondefault configuration. You can do any of the following:

• Define a nondefault address pool for use by a specific interface.

• Define DHCP on an interface even if you have defined local pooling as the global default mechanism.

• Specify one IP address to be assigned to all dial-in peers on an interface.

• Make temporary IP addresses available on a per-interface basis to asynchronous clients using PPP.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. `ip local pool {named-address-pool | default} {first-IP-address [last-IP-address]} [group group-name] [cache-size size]`
4. `interface type number`
5. `peer default ip address pool pool-name-list`
6. `peer default ip address pool dhcp`
7. `peer default ip address ip-address`

**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** `ip local pool {named-address-pool | default} {first-IP-address [last-IP-address] | group group-name} [cache-size size}]` | Creates one or more local IP address pools.  |
| Example: Router(config)# ip local pool default 192.0.2.0 |
| **Step 4** `interface type number` | Specifies the interface and enters interface configuration mode.  |
| Example: Router(config)# interface ethernet 2/0 |
| **Step 5** `peer default ip address pool pool-name-list` | Specifies the pool or pools for the interface to use.  |
| Example: Router(config-if)# peer default ip address pool 2 |
| **Step 6** `peer default ip address pool dhcp` | Specifies DHCP as the IP address mechanism on this interface.  |
| Example: Router(config-if)# peer default ip address pool dhcp |
| **Step 7** `peer default ip address ip-address` | Specifies the IP address to assign to all dial-in peers on an interface.  |
| Example: Router(config-if)# peer default ip address 192.0.2.2 |
Disabling or Reenabling Peer Neighbor Routes

The Cisco IOS software automatically creates neighbor routes by default; that is, it automatically sets up a route to the peer address on a point-to-point interface when the PPP IPCP negotiation is completed.

To disable this default behavior or to reenable it once it has been disabled, perform the following task:

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. no peer neighbor-route
5. peer neighbor-route

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>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Specifies the interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface ethernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no peer neighbor-route</td>
<td>Disables creation of neighbor routes.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# no peer neighbor-route</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> peer neighbor-route</td>
<td>Reenables creation of neighbor routes.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# peer neighbor-route</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Multilink PPP

The Multilink PPP feature provides load balancing functionality over multiple WAN links, while providing multivendor interoperability, packet fragmentation and proper sequencing, and load calculation on both inbound and outbound traffic. The Cisco implementation of MLP supports the fragmentation and packet sequencing specifications in RFC 1990. Additionally, you can change the default endpoint discriminator value that is supplied as part of user authentication. Refer to RFC 1990 for more information about the endpoint discriminator.

MLP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address. The multiple links come up in response to a defined dialer load threshold. The load can be calculated on inbound traffic, outbound traffic, or on either, as needed for the traffic between the specific sites. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

MLP is designed to work over synchronous and asynchronous serial and BRI and PRI types of single or multiple interfaces that have been configured to support both dial-on-demand rotary groups and PPP encapsulation.

Perform the tasks in the following sections, as required for your network, to configure MLP:

Configuring MLP on Synchronous Interfaces

To configure Multilink PPP on synchronous interfaces, you configure the synchronous interfaces to support PPP encapsulation and Multilink PPP.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface serial number
4. no ip address
5. encapsulation ppp
6. ppp multilink
7. pulse-time seconds

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable&lt;br&gt;Example: Router&gt; enable</td>
<td>Enables privileged EXEC mode. • Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal&lt;br&gt;Example: Router&gt; configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface serial number&lt;br&gt;Example:</td>
<td>Specifies an asynchronous interface and enters interface configuration mode.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# interface serial 0/0/1</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**

**Example:**

Router(config-if)# no ip address

*Specifies no IP address for the interface.*

**Step 5**

**Example:**

Router(config-if)# encapsulation ppp

*Enables PPP encapsulation.*

**Step 6**

**Example:**

Router(config-if)# ppp multilink

*Enables Multilink PPP.*

**Step 7**

**Example:**

Router(config-if)# pulse-time 60

*Enables pulsing data terminal ready (DTR) signal intervals on an interface.*

**Note** Repeat these steps for additional synchronous interfaces, as needed.

---

### Configuring a Multilink Group

A multilink group allows you to assign multiple interfaces to a multilink bundle. When the `ppp multilink group` command is configured on an interface, the interface is restricted from joining any interface but the designated multilink group interface. If a peer at the other end of the interface tries to join a different multilink group, the connection is severed. This restriction applies when Multilink PPP (MLP) is negotiated between the local end and the peer system. The interface can still come up as a regular PPP interface.

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface multilink `group-number`
4. ip address `address mask`
5. encapsulation ppp
6. ppp chap hostname `hostname`
7. exit
8. interface `type number`
9. ppp multilink group `group-number`
10. exit
### 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>• Enter your password if prompted.</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 multilink group-number</td>
<td>Creates a multilink bundle and enters interface configuration mode to configure the bundle.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface multilink 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address address mask</td>
<td>Sets a primary IP address for an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip address 192.0.2.1 255.255.255.224</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation ppp</td>
<td>Enables PPP encapsulation.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# encapsulation ppp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ppp chap hostname hostname</td>
<td>Specifies the hostname on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ppp chap hostname host1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> interface type number</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface serial 0/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> ppp multilink group group-number</td>
<td>Restricts a physical link to joining only a designated multilink group interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ppp multilink group 2</td>
<td></td>
</tr>
</tbody>
</table>
PurposeCommand or ActionPurpose

Step 10exitExits interface configuration mode.

Example:

Router(config-if)# exit

Configuring PFC and ACFC

Protocol-Field-Compression (PFC) and Address-and-Control-Field-Compression (AFC) are PPP compression methods defined in RFCs 1661 and 1662. PFC allows for compression of the PPP Protocol field; ACFC allows for compression of the PPP Data Link Layer Address and Control fields.

Configuring ACFC

Follow these steps to configure ACFC handling during PPP negotiation

SUMMARY STEPS

1. enable
2. configure terminal
3. interface multilink number
4. ppp acfc local {request | forbid}
5. ppp acfc remote {apply | reject | ignore}
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1enable</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>Step 2configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3interface multilink number</td>
<td>Select a multilink interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface multilink 2</td>
</tr>
</tbody>
</table>
### Configuring PFC

Follow these steps to configure PFC handling during PPP negotiation:

#### SUMMARY STEPS

1. enable
2. configure terminal
3. interface multilink *number*
4. `ppp pfc local {request | forbid}`
   
   ```
   Router(config-if)# ppp pfc local request
   ```
5. `ppp pfc remote {apply | reject | ignore}`
6. exit

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

Enables privileged EXEC mode.

- Enter your password if prompted.
## PPP and Multilink PPP Configuration

### Purpose

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

**Step 3** | interface multilink *number*  
Example:  
Router(config)# interface multilink 2
| Select a multilink interface.

**Step 4** | ppp pfc local *{request | forbid}*  
Router(config-if)# ppp pfc local request
| Configure how the router handles PFC in its outbound configuration requests where:
  * request—The PFC option is included in outbound configuration requests.
  * forbid—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted.

**Step 5** | ppp pfc remote *{apply | reject | ignore}*  
Example:  
Router(config-if)# ppp pfc remote apply
| Configure a method for the router to use to manage the PFC option in configuration requests received from a remote peer where:
  * apply—PFC options are accepted and PFC may be performed on frames sent to the remote peer.
  * reject—PFC options are explicitly ignored.
  * ignore—PFC options are accepted, but PFC is not performed on frames sent to the remote peer.

**Step 6** | exit  
Example:  
Router(config-if)# exit
| Exits interface configuration mode.

### Changing the Default Endpoint Discriminator

By default, when the system negotiates use of MLP with the peer, the value that is supplied for the endpoint discriminator is the same as the username used for authentication. That username is configured for the interface by the Cisco IOS **ppp chap hostname** or **ppp pap sent-username** command, or defaults to the globally configured hostname (or stack group name, if this interface is a Stack Group Bidding Protocol, or SGBP, group member).

Perform this task to override or change the default endpoint discriminator.

### SUMMARY STEPS

1. enable
### Creating a Multilink Bundle

#### SUMMARY STEPS

1. enable
2. configure terminal
3. interface multilink `group-number`
4. `ip address address mask`
5. encapsulation ppp
6. `ppp multilink`

#### 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>• Enter your password if prompted.</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 virtual template <code>number</code></td>
<td>Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface virtual template 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> `ppp multilink endpoint {hostname</td>
<td>ip ipaddress</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ppp multilink endpoint ip 192.0.2.0</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------------------------</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 multilink group-number</td>
<td>Assigns a multilink group number and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface multilink 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address address mask</td>
<td>Assigns an IP address to the multilink interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip address 192.0.2.9 255.255.255.224</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation ppp</td>
<td>Enables PPP encapsulation.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# encapsulation ppp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ppp multilink</td>
<td>Enables Multilink PPP.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ppp multilink</td>
<td></td>
</tr>
</tbody>
</table>

Assigning an Interface to a Multilink Bundle

⚠️ **Caution**

Do not install a router to the peer address while configuring an MLP lease line. This installation can be disabled when `no ppp peer-neighbor-route` command is used under the MLPPP bundle interface.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface multilink `group-number`
4. `no ip address`
5. keepalive
6. encapsulation ppp
7. ppp multilink `group-number`
8. ppp multilink
9. ppp authentication chap
**10. pulse-time seconds**

### 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.  
Example:  
`Router> enable`  
- Enter your password if prompted. |
| **Step 2** | `configure terminal` | Enters global configuration mode.  
Example:  
`Router# configure terminal` |
| **Step 3** | `interface multilink group-number` | Assigns a multilink group number and enters interface configuration mode.  
Example:  
`Router(config)# interface multilink 10` |
| **Step 4** | `no ip address` | Removes any specified IP address.  
Example:  
`Router(config-if)# no ip address` |
| **Step 5** | `keepalive` | Sets the frequency of keepalive packets.  
Example:  
`Router(config-if)# keepalive` |
| **Step 6** | `encapsulation ppp` | Enables PPP encapsulation.  
Example:  
`Router(config-if)# encapsulation ppp` |
| **Step 7** | `ppp multilink group group-number` | Restricts a physical link to joining only the designated multilink-group interface.  
Example:  
`Router(config-if)# ppp multilink 12` |
| **Step 8** | `ppp multilink` | Enables Multilink PPP.  
Example:  
`Router(config-if)# ppp multilink` |
| **Step 9** | `ppp authentication chap` | (Optional) Enables CHAP authentication.  
Example:  
`Router(config-if)# ppp authentication chap` |
**Configuring PPP/MLP MRRU Negotiation Configuration on Multilink Groups**

In this task, you configure MRRU negotiation on the multilink interface. The bundle interface is static, that is, always available.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface multilink number**
4. **ip address ip-address mask**
5. **ppp multilink mrru [local | remote] mrru-value**
6. **mtu bytes**
7. **exit**
8. **interface serial slot/port**
9. **ppp multilink**
10. **ppp multilink group group-number**
11. **mtu bytes**
12. **exit**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>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&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></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>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>interface multilink number</td>
<td>Creates a virtual template interface that can be configured</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>and applied dynamically in creating virtual access</td>
</tr>
<tr>
<td>Router(config)# interface multilink 10</td>
<td>interfaces, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>4</td>
<td><strong>ip address ip-address mask</strong>&lt;br&gt;Example: &lt;br&gt;Router(config-if)# ip address 10.13.1.1 255.255.255.0</td>
</tr>
<tr>
<td>5</td>
<td>**ppp multilink mrru [local</td>
</tr>
<tr>
<td></td>
<td><strong>local</strong>—(Optional) Configures the local MRRU value. &lt;br&gt;The default values for the local MRRU are the value of the multilink group interface MTU for multilink group members, and 1524 bytes for all other interfaces.</td>
</tr>
<tr>
<td></td>
<td><strong>remote</strong>—(Optional) Configures the minimum value that the software will accept from the peer when it advertises its MRRU. By default, the software accepts any peer MRRU value of 128 or higher. You can specify a higher minimum acceptable MRRU value in a range from 128 to 16384 bytes.</td>
</tr>
<tr>
<td>6</td>
<td><strong>mtu bytes</strong>&lt;br&gt;Example: &lt;br&gt;Router(config-if)# mtu 1600</td>
</tr>
<tr>
<td></td>
<td><strong>Once you configure the MRRU on the bundle interface, you enable the router to receive large reconstructed MLP frames. You may want to configure the bundle MTU so the router can transmit large MLP frames, although it is not strictly necessary.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>The maximum recommended value for the bundle MTU is the value of the peer’s MRRU. The default MTU for serial interfaces is 1500. The software will automatically reduce the bundle interface MTU if necessary, to avoid violating the peer’s MRRU.</strong></td>
</tr>
<tr>
<td>7</td>
<td><strong>exit</strong>&lt;br&gt;Example: &lt;br&gt;Router(config-if)# exit</td>
</tr>
<tr>
<td>8</td>
<td><strong>interface serial slot/port</strong>&lt;br&gt;Example: &lt;br&gt;Router(config)# interface serial 0/0</td>
</tr>
<tr>
<td>9</td>
<td><strong>ppp multilink</strong>&lt;br&gt;Example:</td>
</tr>
</tbody>
</table>
### PPP and Multilink PPP Configuration

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# ppp multilink</td>
<td></td>
</tr>
</tbody>
</table>

**Step 10**

**ppp multilink group group-number**

**Example:**

Router(config-if)# ppp multilink group 1

Restricts a physical link to joining only a designated multilink-group interface.

**Step 11**

**mtu bytes**

**Example:**

Router(config-if)# mtu 1600

(Optional) Adjusts the maximum packet size or MTU size.

- The default MTU for serial interfaces is 1500.
- When the bundle interface MTU is tuned to a higher number, then depending upon the fragmentation configuration, the link interface may be given larger frames to transmit.
- You must ensure that fragmentation is performed such that fragments are sized less than the link interface MTU (refer to command pages for the ppp multilink fragmentation and ppp multilink fragment-delay commands for more information about packet fragments), or configure the MTUs of the link interfaces such that they can transmit the larger frames.

**Step 12**

**exit**

**Example:**

Router(config-if)# exit

Exits interface configuration mode and returns to global configuration mode.

### Disabling PPP Multilink Fragmentation

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface multilink group-number
4. ppp multilink fragment disable
5. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 1</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 1</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
### Troubleshooting Tips

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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 multilink group-number</td>
<td>Assigns a multilink group number and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# interface multilink 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ppp multilink fragment disable</td>
<td>(Optional) Disables PPP multilink fragmentation.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# ppp multilink fragment disable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting Tips**

Use the `debug ppp negotiation` command to verify and troubleshoot MRRU negotiation on multilink groups. Use the `show interface` command to verify MRRU negotiation on the interfaces.

For more information about configuring MRRU and MTU values, see the *Wide-Area Networking Configuration Guide: Multilink PPP, Cisco IOS XE Release 3S*.

**Troubleshooting PPP**

You can troubleshoot PPP reliable link by using the `debug lapb` command and the `debug ppp negotiations`, `debug ppp errors`, and `debug ppp packets` commands. You can determine whether Link Access Procedure, Balanced (LAPB) has been established on a connection by using the `show interface` command.

**Monitoring and Maintaining PPP and MLP Interfaces**

You can use the `show ppp multilink` command to display MLP bundle information.

For more information about configuring MLPPP interfaces, see the *Wide-Area Networking Configuration Guide: Multilink PPP, Cisco IOS XE Release 3S*. 
Configuring Raw Socket Transport on the Cisco ASR 903 Router

Note

Raw Socket Transport Configuration is not supported on the Cisco ASR 900 RSP3 module.

This document describes how to configure Raw Socket on the Cisco ASR 903 Router.

Note

This feature requires the use of a serial interface module, which is not included with the Cisco ASR 903 router.

Understanding Raw Socket Transport

Raw Socket Transport is a method for transporting serial data through an IP network. Raw Socket transports Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs). This method is an alternative to the Block Serial Tunnel (BSTUN) protocol. Raw Socket supports point-to-point and point-to-multipoint connections.

Raw Socket Transport supports point-to-multipoint connection over an asynchronous serial line and has a built-in auto TCP connection retry mechanism.

Raw Socket Transport supports the following for each serial interface:

- Up to 32 TCP session per interface
- Interface configuration as a server, client, or a combination of both.
- One server per interface, but multiple clients.

Using the Cisco ASR 903 Router with the serial interface module allows you to transport Raw Socket data over a variety of protocols, including global routing, MPLS VPN, and VRF Lite.
Figures below show example topologies for raw socket using the Cisco ASR 903 Router with the serial interface module.

Raw Socket Configuration

The following sections describe how to configure Raw Socket on the Cisco ASR 903 Router with the serial interface module.

Configuring a Raw Socket Server with Global Routing Table

Use the following steps to configure the Cisco ASR 903 Router as a Raw Socket server using the global routing table.

SUMMARY STEPS

1. configure terminal
2. interface serial slot/subslot/port
3. no ip address
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface serial slot/subslot/port</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>no ip address</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
</tbody>
</table>

Example:

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

Exit interface configuration mode.

• Repeat Step 2 through Step 4 to create additional serial interfaces.

Note

1. line [aux | console | tty | vty] line-ifc-number [ending-line-ifc-number]

```
Router(config)# line 0/1/0
```

Identifies a specific line or range of lines for configuration and enters line configuration mode.

1. raw-socket tcp server port [ip_address]
Router(config-line)# raw-socket tcp server 5000 10.1.1.1

Starts the Raw Socket TCP server for a line interface.

1. exit

Exits line configuration mode.

1. interface Loopback number

Router(config)# interface loopback0

Enters configuration mode on the loopback interface.

1. ip address ip-address mask

Router(config-if)# ip address 10.1.1.1 255.255.255.255

Specifies an IP address for the loopback address.

1. exit

Exits interface configuration mode.

1. router isis [area-tag]


1. net net1 alt net2

Configures an Intermediate System-to-Intermediate System (IS-IS) network entity table (NET) for the routing process.

1. passive-interface [default] interface-type interface-number

Router(config-router)# passive-interface Loopback0

Disables transmission of routing updates on the loopback interface.

1. end

Exit configuration mode.

1. Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.
Configuring a Raw Socket Client with Global Routing Table

Use the following steps to configure the Cisco ASR 903 Router as a Raw Socket client using the global routing table.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface serial slot/subslot/port`
3. `no ip address`
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface serial slot/subslot/port</td>
<td>Enters configuration mode for the serial interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong> no ip address</td>
<td>Disables IP processing on the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exit interface configuration mode.</td>
</tr>
</tbody>
</table>

- Repeat Step 2 through Step 4 to create additional serial interfaces.

1. `end`

Exit configuration mode.

1. `line [aux | console | tty | vty] line-ifc-number [ending-line-ifc-number]`

`Router(config)# line 0/1/0`

Identifies a specific line for configuration and enters line configuration collection mode.

1. `raw-socket tcp client dest_ip_address dest_port [local_ip_address] [local_port]`

`Router(config-line)# raw-socket tcp client 10.1.1.1 5000 172.2.2.2 9000`

Initiates a Raw Socket TCP client session.

1. `exit`

Repeat Step 6 through Step 8 to create additional line interfaces.

1. `interface loopback number`

`Router(config)# interface loopback0`
Enters configuration mode on the loopback interface.
1. **ip address ip-address mask**

   ```
   Router(config-if)# ip address 172.2.2.2 255.255.255.255
   ```

Specifies an IP address for the loopback address.
1. **exit**

Exits interface configuration mode.
1. **router isis [area-tag]**

1. **net net1 alt net2**

   ```
   Router(config-router)# net 47.0004.004d.0001.0001.0c11.1111.00
   ```

Configures an Intermediate System-to-Intermediate System (IS-IS) network entity table (NET) for the routing process.
1. **passive-interface [default] interface-type interface-number**

   ```
   Router(config)# passive-interface Loopback0
   ```

Disables transmission of routing updates on the loopback interface.
1. **end**

Exit configuration mode.
1. **linecode {ami | b8zs | hdb3}**

Selects the linecode type.
   - `ami`—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
   - `b8zs`—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
   - `hdb3`—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

---

**Configuring Raw Socket Server with MPLS VPN**

Use the following steps to configure the Cisco ASR 903 Router as a Raw Socket server using MPLS VPN.

**SUMMARY STEPS**

1. **configure terminal**
2. **vrf definition vrf-name**
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>vrf definition vrf-name</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configures a virtual routing and forwarding (VRF) routing table instance and enters VRF configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>rd route-distinguisher</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies a route distinguisher (RD) to distribute endpoint information in a Virtual Private LAN Service (VPLS) configuration.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>address-family ipv4 [unicast] vrf vrf-name</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>router-target import</td>
<td>export</td>
</tr>
<tr>
<td>Example: ROUTER (config)# route-target export 101:3</td>
<td>Configures the Virtual Private LAN Services (VPLS) virtual forwarding instance (VFI) to export routing information to the target VPN extended community.</td>
</tr>
<tr>
<td>Step 7 route-target import</td>
<td>export</td>
</tr>
<tr>
<td>Example: ROUTER (config)# route-target import 101:3</td>
<td>Configures the Virtual Private LAN Services (VPLS) virtual forwarding instance (VFI) to import routing information from the target VPN extended community.</td>
</tr>
<tr>
<td>Step 8 exit-address-family</td>
<td>Exits address-family configuration mode.</td>
</tr>
<tr>
<td>Step 9 interface serial slot/subslot/port</td>
<td>Enters configuration mode for the serial interface.</td>
</tr>
<tr>
<td>Step 10 vrf forwarding vrf-name [downstream vrf-name2]</td>
<td>Step 10</td>
</tr>
<tr>
<td>Example: ROUTER (config-if)# vrf forwarding scada</td>
<td>Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface.</td>
</tr>
<tr>
<td>Step 11 no ip address</td>
<td>Step 11</td>
</tr>
<tr>
<td>Example: ROUTER (config)# interface loopback0</td>
<td>Disables IP processing on the interface.</td>
</tr>
<tr>
<td>Step 12 exit</td>
<td>Step 12</td>
</tr>
<tr>
<td>Example: ROUTER (config)# interface loopback0</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td>Step 13 interface Loopback number</td>
<td>Step 13</td>
</tr>
<tr>
<td>Example: ROUTER (config)# interface loopback0</td>
<td>Enters configuration mode on the loopback interface.</td>
</tr>
<tr>
<td>Step 14 vrf forwarding vrf-name [downstream vrf-name2]</td>
<td>Step 14</td>
</tr>
<tr>
<td>Example: ROUTER (config)# vrf forwarding scada</td>
<td>Configuring Raw Socket Transport on the Cisco ASR 903 Router</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>15</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>16</td>
<td>exit</td>
</tr>
<tr>
<td>17</td>
<td>router bgp autonomous-system-number</td>
</tr>
<tr>
<td>18</td>
<td>address-family vpnv4 [multicast</td>
</tr>
<tr>
<td>19</td>
<td>address-family ipv4 [unicast] vrf vrf-name</td>
</tr>
<tr>
<td>20</td>
<td>redistribute connected</td>
</tr>
<tr>
<td>21</td>
<td>exit-address-family</td>
</tr>
<tr>
<td>22</td>
<td>end</td>
</tr>
<tr>
<td>23</td>
<td>linecode {ami</td>
</tr>
</tbody>
</table>
### Configuring a Raw Socket Client with MPLS VPN

Use the following steps to configure the Cisco ASR 903 Router as a Raw Socket client using MPLS VPN.

#### SUMMARY STEPS

1. `configure terminal`
2. `vrf definition vrf-name`
3. `rd route-distinguisher`
4. `address-family ipv4 [unicast] vrf vrf-name`
5. `route-target [import | export | both] route-target-ext-community`
6. `route-target [import | export | both] route-target-ext-community`
7. `exit-address-family`
8. `interface serial slot/subslot/port`
9. `vrf forwarding vrf-name [downstream vrf-name2]`
10. `no ip address`
11. `exit`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Enters configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>vrf definition vrf-name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# vrf definition scada</td>
<td></td>
</tr>
<tr>
<td>Configures a virtual routing and forwarding (VRF) routing table instance and enters VRF configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>rd route-distinguisher</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-vrf)# rd 101:3</td>
<td></td>
</tr>
<tr>
<td>Specifies a route distinguisher (RD) to distribute endpoint information in a Virtual Private LAN Service (VPLS) configuration.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>address-family ipv4 [unicast] vrf vrf-name</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# address-family ipv4</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>`route-target [import</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Router(config-router-af)# route-target export 101:3</code></td>
</tr>
<tr>
<td>Step 6</td>
<td>`route-target [import</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Router(config-router-af)# route-target import 101:3</code></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>exit-address-family</code></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>interface serial slot/subslot/port</code></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>vrf forwarding vrf-name [downstream vrf-name2]</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# vrf forwarding scada</code></td>
</tr>
<tr>
<td>Step 10</td>
<td><code>no ip address</code></td>
</tr>
<tr>
<td>Step 11</td>
<td><code>exit</code></td>
</tr>
</tbody>
</table>
**Note**

• Repeat Step 8 through Step 11 to create additional serial interfaces.

1. **line [aux | console | tty | vty] line-ifc-number [ending-line-ifc-number]**

   Router(config)# line 0/1/0

Identifies a specific line for configuration and enters line configuration collection mode.

1. **raw-socket tcp client dest_ip_address dest_port [local_ip_address] [local_port]**

   Router(config-line)# raw-socket tcp client 10.1.1.1 5000 172.2.2.2 9000

Initiates a Raw Socket TCP client session.

1. **exit**

   Exits line configuration mode.

**Note**

• Repeat Step 6 through Step 8 to create additional line interfaces.

1. **interface Loopback number**

   Router(config)# interface loopback0

Enters configuration mode on the loopback interface.

1. **vrf forwarding vrf-name [downstream vrf-name2]**

   Router(config-if)# vrf forwarding scada

Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface.

1. **ip address ip-address mask**

   Router(config-if)# ip address 172.2.2.2 255.255.255.255

Specifies an IP address for the loopback interface.

1. **exit**

   Exits interface configuration mode.

1. **router bgp autonomous-system-number**

   Router(config-router)# router bgp 1111

Configures a Border Gateway Protocol (BGP) routing process.

1. **address-family vpnv4 [multicast | unicast]**
Enters address family configuration mode to configure a routing session using Virtual Private Network (VPN) Version 4 address prefixes

1. **address-family ipv4 [unicast] vrf vrf-name**

Enters the address family submode for configuring routing protocols.

1. **redistribute connected**

Configures the router to redistribute routes from one routing domain into another routing domain.

1. **exit-address-family**

Exits address-family configuration mode.

1. **end**

Exit configuration mode.

1. **linecode {ami | b8zs | hdb3}**

Selects the linecode type.

- `ami`—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- `b8zs`—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- `hdb3`—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

---

**Configuring a Raw Socket Server with VRF Lite**

Use the following steps to configure the Cisco ASR 903 Router as a Raw Socket server using VRF Lite.

**SUMMARY STEPS**

1. **configure terminal**
2. **vrf definition vrf-name**
3. **rd route-distinguisher**
4. **address-family ipv4 [unicast] vrf vrf-name**
5. **route-target [import | export | both] route-target-ext-community**
6. **route-target [import | export | both] route-target-ext-community**
7. **exit-address-family**
8. **interface serial slot/subslot/port**
9. **vrf forwarding vrf-name [downstream vrf-name2]**
10. **no ip address**
11. **exit**
12. `line [aux | console | tty | vty] line-ifc-number [ending-line-ifc-number]`
13. `raw-socket tcp server port [ip_address]`
14. `exit`
15. `interface GigabitEthernet slot /subslot /port`
16. `encapsulation dot1q vlan-id`
17. `vrf forwarding vrf-name [downstream vrf-name2]`
18. `ip address ip-address mask`
19. `exit`
20. `router bgp autonomous-system-number`
21. `address-family ipv4 [unicast] vrf vrf-name`
22. `redistribute connected`
23. `neighbor { ip-address | ipv6-address% | peer-group-name } remote-as autonomous-system-number [ alternate-as autonomous-system-number ... ]`
24. `neighbor { ip-address | peer-group-name | ipv6-address% } activate` Router(config-router-af)# neighbor 10.1.1.2 activate
25. `exit-address-family`
26. `end`
27. `linecode {ami | b8zs | hdb3}

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>vrf definition vrf-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# vrf definition scada</td>
<td>Configures a virtual routing and forwarding (VRF) routing table instance and enters VRF configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>rd route-distinguisher</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-vrf)# rd 100:3</td>
<td>Specifies a route distinguisher (RD) to distribute endpoint information in a Virtual Private LAN Service (VPLS) configuration.</td>
</tr>
<tr>
<td>Step 4</td>
<td>address-family ipv4 [unicast] vrf vrf-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# address-family ipv4</td>
<td>Enters the address family submode for configuring routing protocols.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>route-target [import</td>
<td>export</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-router-af)# route-target export 100:3</td>
<td>Configures the Virtual Private LAN Services (VPLS) virtual forwarding instance (VFI) to export routing information to the target VPN extended community.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>route-target [import</td>
<td>export</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-router-af)# route-target import 100:3</td>
<td>Configures the Virtual Private LAN Services (VPLS) virtual forwarding instance (VFI) to import routing information from the target VPN extended community.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit-address-family</td>
<td>Exits address-family configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>interface serial slot/subslot/port</td>
<td>Enters configuration mode for the serial interface.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>vrf forwarding vrf-name [downstream vrf-name2]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# vrf forwarding scada</td>
<td>Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>no ip address</td>
<td>Disables IP processing on the interface.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>line [aux</td>
<td>console</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config)# line 0/1/0</td>
<td>Identifies a specific line for configuration and enters line configuration collection mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>raw-socket tcp server port [ip_address]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# raw-socket tcp server 5000 10.1.1.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Starts the Raw Socket TCP server for a line interface.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>Start the Raw Socket TCP server for a line interface.</td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Exits line configuration mode.</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>Exits line configuration mode.</td>
</tr>
<tr>
<td><strong>interface GigabitEthernet slot/subslot/port</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface GigabitEthernet0/10</td>
<td>Enters configuration mode on the Gigabit Ethernet interface.</td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td>Enters configuration mode on the Gigabit Ethernet interface.</td>
</tr>
<tr>
<td><strong>encapsulation dot1q vlan-id</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# encapsulation dot1q 10</td>
<td>Enables IEEE 802.1Q encapsulation of traffic on the interface.</td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td>Enables IEEE 802.1Q encapsulation of traffic on the interface.</td>
</tr>
<tr>
<td><strong>vrf forwarding vrf-name [downstream vrf-name2]</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# vrf forwarding scada</td>
<td>Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface.</td>
</tr>
<tr>
<td><strong>Step 18</strong></td>
<td>Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface.</td>
</tr>
<tr>
<td><strong>ip address ip-address mask</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip address 10.1.1.1 255.255.255.0</td>
<td>Specifies an IP address for the Gigabit Ethernet interface.</td>
</tr>
<tr>
<td><strong>Step 19</strong></td>
<td>Specifies an IP address for the Gigabit Ethernet interface.</td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 20</strong></td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td><strong>router bgp autonomous-system-number</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-router)# router bgp 100</td>
<td>Configures a Border Gateway Protocol (BGP) routing process.</td>
</tr>
<tr>
<td><strong>Step 21</strong></td>
<td>Configures a Border Gateway Protocol (BGP) routing process.</td>
</tr>
<tr>
<td><strong>address-family ipv4 [unicast] vrf vrf-name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# address-family ipv4 vrf scada</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enters the address</td>
<td>Configures the router to redistribute routes from one</td>
</tr>
<tr>
<td>family submode for</td>
<td>another routing domain</td>
</tr>
<tr>
<td>configuring routing</td>
<td></td>
</tr>
<tr>
<td>protocols.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 22</strong></td>
<td><strong>redistribute connected</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Step 23**            | **neighbor** { ip-address | ipv6-address% | peer-group-name }** \**
|                        | **remote-as** autonomous-system-number [ alternate-as autonomous-system-number ... ]** \**
|                        | **Example:**                                                            |
|                        | Router(config-router-af)# neighbor 10.1.1.2                             |
|                        | remote-as 1111                                                          |
|                        | Adds an entry to the BGP or multiprotocol BGP neighbor table.           |
| **Step 24**            | **neighbor** { ip-address | peer-group-name | ipv6-address% }\** activate** \**
|                        | Router(config-router-af)# neighbor 10.1.1.2 activate                   |
|                        | Enables the exchange of information with a Border Gateway Protocol (BGP) neighbor. |
| **Step 25**            | **exit-address-family**                                                |
|                        | Exits address-family configuration mode.                               |
| **Step 26**            | **end**                                                                |
|                        | Exit configuration mode.                                               |
| **Step 27**            | **linecode** { ami | b8zs | hdb3}                                  |
|                        | Selects the linecode type.                                             |
|                        | • ami—Specifies Alternate Mark Inversion (AMI) as the linecode type.    |
|                        | Valid for T1 and E1 controllers.                                       |
|                        | • b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type.|
|                        | Valid for sonet controller only. This is the default for T1 lines.    |
|                        | • hdb3—Specifies high-density binary 3 (hdb3) as the linecode type.     |
|                        | Valid for E1 controller only. This is the default for E1 lines.        |

### Configuring a Raw Socket Client with VRF Lite

Use the following steps to configure the Cisco ASR 903 Router as a Raw Socket client using VRF Lite.

#### SUMMARY STEPS

1. `configure terminal`
2. `vrf definition vrf-name`
3. `rd route-distinguisher`
4. `address-family ipv4 [unicast]`
5. `route-target [import | export | both] route-target-ext-community`
6. `route-target [import | export | both] route-target-ext-community`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>vrf definition vrf-name</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>rd route-distinguisher</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>address-family ipv4 [unicast]</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**route-target [import</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>**route-target [import</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit-address-family</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>interface serial slot/subslot/port</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>vrf forwarding vrf-name [downstream vrf-name2]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# vrf forwarding scada</td>
</tr>
<tr>
<td></td>
<td>Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>no ip address</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>exit</td>
</tr>
</tbody>
</table>

Exits interface configuration mode.

**Note**
- Repeat **Step 8** through **Step 11** to create additional serial interfaces.

1. `line [aux | console | tty | vty] line-ifc-number [ending-line-ifc-number]`
   
   Router(config)# line 0/1/0

Identifies a specific line for configuration and enters line configuration collection mode.

1. `raw-socket tcp client dest_ip_address dest_port [local_ip_address] [local_port]`
   
   Router(config-line)# raw-socket tcp client 10.1.1.1 5000 172.1.1.1 9000

Initiates a Raw Socket TCP client session.

1. exit

Exits line configuration mode.

**Note**
- Repeat **Step 12** through **Step 16** to create additional line interfaces.

1. `interface GigabitEthernet slot/subslot/port`
   
   Router(config)# interface GigabitEthernet0/0/0

Enters configuration mode on the Gigabit Ethernet interface.

1. `encapsulation dot1q vlan-id`
   
   Router(config-if)# encapsulation dot1q 10
Enables IEEE 802.1Q encapsulation of traffic on the interface.

1. `vrf forwarding vrf-name [downstream vrf-name2]`

   ```
   Router(config-if)# vrf forwarding scada
   ```

Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface.

1. `ip address ip-address mask`

   ```
   Router(config-if)# ip address 172.1.1.1 255.255.255.0
   ```

Specifies an IP address for the Gigabit Ethernet interface.

1. `exit`

Exits interface configuration mode.

1. `router bgp autonomous-system-number`

   ```
   Router(config-router)# router bgp 200
   ```

Configures a Border Gateway Protocol (BGP) routing process.

1. `address-family ipv4 [unicast] vrf vrf-name`

   ```
   Router(config)# address-family ipv4 vrf scada
   ```

Enters the address family submode for configuring routing protocols.

1. `redistribute connected`

Configures the router to redistribute routes from one routing domain into another routing domain.

1. `neighbor { ip-address | ipv6-address | peer-group-name } remote-as autonomous-system-number [ alternate-as autonomous-system-number ... ]`

   ```
   Router(config-router-af)# neighbor 172.1.1.2 remote-as 1111
   ```

Adds an entry to the BGP or multiprotocol BGP neighbor table.

1. `neighbor { ip-address | peer-group-name | ipv6-address% } activate` 

   ```
   Router(config-router-af)# neighbor 172.1.1.2 activate
   ```

Enables the exchange of information with a Border Gateway Protocol (BGP) neighbor.

1. `exit-address-family`

Exits address-family configuration mode.

1. `end`

Exit configuration mode.

1. `linecode {ami | b8zs | hdb3}`
Selects the linecode type.

- **ami**—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- **b8zs**—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- **hdb3**—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

### Line Commands

Table below summarizes commands that you can apply to lines.

**Table 6: Line Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>databits</strong> {5</td>
<td>6</td>
</tr>
<tr>
<td>**line [aux</td>
<td>console</td>
</tr>
</tbody>
</table>
| ```bash
Router(config)# line 0/1/0
```                                           |                                                                                             |
| **parity** {none | even | odd | space | mark}                                        | Configures the router to generate a parity bit. The default value is none.                 |
| **raw-socket packet-length** packet_size     | Sets the packet length that the serial driver uses to packetize the serial bytes into TCP frames. Valid values are 2–1400 and indicate bytes. |
| ```bash
Router(config-line)# raw-socket packet-length 32
```                                           | **Note** The packet length must be configured, else the feature may not work.               |
| **raw-socket packet-timer** packet_timer     | Sets the packet timer that the serial driver uses when packetizing serial bytes into TCP frames. Values are in milliseconds. |
| ```bash
Router(config-line)# raw-socket packet-timer 3
```                                           |                                                                                             |
| **raw-socket special-char** special_character| (Optional) Sets the special character that triggers the packetization of incoming bytes.     |
| ```bash
Router(config-line)# raw-socket special-char 10
```                                          |                                                                                             |
| **raw-socket tcp idle-timeout** session_timeout| Sets the Raw Socket TCP session timeout for a line interface. By default, the session idle timeout is 5 minutes. |
| ```bash
Router(config-line)# raw-socket tcp idle-timeout 5
```                                          |                                                                                             |
| **raw-socket tcp server** port [ ip_address ] | Starts the Raw Socket TCP server for a line interface.                                      |
| ```bash
Router(config-line)# raw-socket tcp server 5000 10.1.1.1
```                                         |                                                                                             |
Configure the transmit and receive speed of a line interface. Valid values are in bps and include 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 28800, 32000, 8400, 48000, 56000, 57600, 64000, 72000, 115200, 128000, and 230400 bps.

The default value is 9600 bps.

Sets the number of the stop bits transmitted per byte. The default value is 2.

Selects the line code type.

- **ami**—Specifies Alternate Mark Inversion (AMI) as the line code type. Valid for T1 and E1 controllers.
- **b8zs**—Specifies binary 8-zero substitution (B8ZS) as the line code type. Valid for sonet controller only. This is the default for T1 lines.
- **hdb3**—Specifies high-density binary 3 (hdb3) as the line code type. Valid for E1 controller only. This is the default for E1 lines.

### Troubleshooting Commands

You can use the following commands to display information for troubleshooting raw socket:

- **clear raw-socket tcp**—Clears Raw Socket TCP statistics for a specific TTY interface or for all asynchronous interfaces.
- **debug raw-socket driver event**—Enables Raw Socket driver event debugging.
- **debug raw-socket driver packet**—Enables debugging for issues related to Raw Socket driver packets.
- **debug raw-socket tcp event**—Enables debugging for issues related to Raw Socket TCP sessions
- **debug raw-socket tcp packet**—raw TCP packets at the socket level
- **show raw-socket tcp detail**—Displays the details of Raw Socket TCP activity, mainly for debugging purposes
- **show raw-socket tcp sessions**—Displays Raw Socket TCP session details
- **show raw-socket tcp statistic**—Displays Raw Socket TCP statistics for each asynchronous interface

### Sample Show Command Output

The following examples contain output from these commands.

Router# show raw-socket tcp detail
Line 00, if: 0/0/0 tty: 3, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 0, l_ip: 10.0.0.68, l_port: 1, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 01, if: 0/0/1 tty: 4, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 1, l_ip: 10.0.0.68, l_port: 2, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 02, if: 0/0/2 tty: 5, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 2, l_ip: 10.0.0.68, l_port: 3, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 03, if: 0/0/3 tty: 6, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 3, l_ip: 10.0.0.68, l_port: 4, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 04, if: 0/0/4 tty: 7, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 4, l_ip: 10.0.0.68, l_port: 5, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 05, if: 0/0/5 tty: 8, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 5, l_ip: 10.0.0.68, l_port: 6, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 06, if: 0/0/6 tty: 9, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 6, l_ip: 10.0.0.68, l_port: 7, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 07, if: 0/0/7 tty: 10, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 7, l_ip: 10.0.0.68, l_port: 8, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 08, if: 0/1/0 tty: 19, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 8, l_ip: 10.0.0.68, l_port: 9, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 09, if: 0/1/1 tty: 20, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 9, l_ip: 10.0.0.68, l_port: 10, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 10, if: 0/1/2 tty: 21, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 10, l_ip: 10.0.0.68, l_port: 11, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 11, if: 0/1/3 tty: 22, server status: off, socket: ---, listen port: ----, total sessions: 1
<--[out] Session 0, socket: 11, l_ip: 10.0.0.68, l_port: 12, d_ip: 172.1.1.1, d_port: 1 w_err: 0
Line 12, if: ---- tty: ---, server status: off, socket: ---, listen port: ----, total sessions: 0
Line 13, if: ---- tty: ---, server status: off, socket: ---, listen port: ----, total sessions: 0
Line 14, if: ---- tty: ---, server status: off, socket: ---, listen port: ----, total sessions: 0
Line 15, if: ---- tty: ---, server status: off, socket: ---, listen port: ----, total sessions: 0
Line 16, if: ---- tty: ---, server status: off, socket: ---, listen port: ----, total sessions: 0
Line 17, if: ---- tty: ---, server status: off, socket: ---, listen port: ----, total sessions: 0
Line 18, if: ---- tty: ---, server status: off, socket: ---, listen port: ----, total sessions: 0
Line 19, if: ---- tty: ---, server status: off, socket: ---, listen port: ----, total sessions: 0
Line 20, if: ---- tty: ---, server status: off, socket: ---, listen port: ----, total sessions: 0
### Socket Mapping

<table>
<thead>
<tr>
<th>Socket status</th>
<th>interface</th>
<th>hwidb</th>
<th>local_ip_addr</th>
<th>local_port</th>
<th>dest_ip_addr</th>
<th>dest_port</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>0/0/0</td>
<td>3</td>
<td>29C1CA98</td>
<td>10.0.0.68</td>
<td>1 172.1.1.11</td>
<td>1</td>
</tr>
<tr>
<td>connected</td>
<td>0/0/1</td>
<td>4</td>
<td>29C1D7FC</td>
<td>10.0.0.68</td>
<td>2 172.1.1.11</td>
<td>1</td>
</tr>
<tr>
<td>connected</td>
<td>0/0/2</td>
<td>5</td>
<td>31156BBC</td>
<td>10.0.0.68</td>
<td>3 172.1.1.11</td>
<td>1</td>
</tr>
<tr>
<td>connected</td>
<td>0/0/3</td>
<td>6</td>
<td>2A36BFF0</td>
<td>10.0.0.68</td>
<td>4 172.1.1.11</td>
<td>1</td>
</tr>
<tr>
<td>connected</td>
<td>0/0/4</td>
<td>7</td>
<td>411EE10</td>
<td>10.0.0.68</td>
<td>5 172.1.1.11</td>
<td>1</td>
</tr>
<tr>
<td>connected</td>
<td>0/0/5</td>
<td>8</td>
<td>29C20C28</td>
<td>10.0.0.68</td>
<td>6 172.1.1.11</td>
<td>1</td>
</tr>
<tr>
<td>connected</td>
<td>0/0/6</td>
<td>9</td>
<td>29C2198C</td>
<td>10.0.0.68</td>
<td>7 172.1.1.11</td>
<td>1</td>
</tr>
<tr>
<td>connected</td>
<td>0/0/7</td>
<td>10</td>
<td>3115987C</td>
<td>10.0.0.68</td>
<td>8 172.1.1.11</td>
<td>1</td>
</tr>
<tr>
<td>connected</td>
<td>0/0/8</td>
<td>19</td>
<td>2A36EE40</td>
<td>10.0.0.68</td>
<td>9 172.1.1.11</td>
<td>1</td>
</tr>
<tr>
<td>connected</td>
<td>0/0/9</td>
<td>20</td>
<td>319D668C</td>
<td>10.0.0.68</td>
<td>10 172.1.1.11</td>
<td></td>
</tr>
<tr>
<td>connected</td>
<td>0/1/0</td>
<td>21</td>
<td>29C2A388</td>
<td>10.0.0.68</td>
<td>11 172.1.1.11</td>
<td></td>
</tr>
<tr>
<td>connected</td>
<td>0/1/1</td>
<td>22</td>
<td>41B40454</td>
<td>10.0.0.68</td>
<td>12 172.1.1.11</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Event List

<table>
<thead>
<tr>
<th>Event_addr</th>
<th>initiator event_action</th>
<th>local_ip_addr</th>
<th>local_port</th>
<th>dest_ip_addr</th>
<th>dest_port</th>
<th>retry_count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x30E28C2C</td>
<td>start client</td>
<td>1 172.1.1.11</td>
<td>1 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x30E28BC4</td>
<td>start client</td>
<td>2 172.1.1.11</td>
<td>1 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x30E28B5C</td>
<td>start client</td>
<td>3 172.1.1.11</td>
<td>1 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x30E28AF4</td>
<td>start client</td>
<td>4 172.1.1.11</td>
<td>1 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x30E28A8C</td>
<td>start client</td>
<td>5 172.1.1.11</td>
<td>1 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x30E28A24</td>
<td>start client</td>
<td>6 172.1.1.11</td>
<td>1 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x30E28B4</td>
<td>start client</td>
<td>7 172.1.1.11</td>
<td>1 0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Sample Show Command Output

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Local IP Addr</th>
<th>Local Port</th>
<th>Dest IP Addr</th>
<th>Dest Port</th>
<th>Up Time</th>
<th>Idle Time/Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/0/0</td>
<td>3 0</td>
<td>10.0.0.68</td>
<td>1</td>
<td>172.1.1.1</td>
<td>1</td>
<td>02:00:37</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/0/1</td>
<td>4 1</td>
<td>10.0.0.68</td>
<td>2</td>
<td>172.1.1.1</td>
<td>1</td>
<td>02:00:37</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/0/2</td>
<td>5 2</td>
<td>10.0.0.68</td>
<td>3</td>
<td>172.1.1.1</td>
<td>1</td>
<td>02:00:37</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/0/3</td>
<td>6 3</td>
<td>10.0.0.68</td>
<td>4</td>
<td>172.1.1.1</td>
<td>1</td>
<td>02:00:37</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/0/4</td>
<td>7 4</td>
<td>10.0.0.68</td>
<td>5</td>
<td>172.1.1.1</td>
<td>1</td>
<td>02:00:37</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/0/5</td>
<td>8 5</td>
<td>10.0.0.68</td>
<td>6</td>
<td>172.1.1.1</td>
<td>1</td>
<td>02:00:37</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/0/6</td>
<td>9 6</td>
<td>10.0.0.68</td>
<td>7</td>
<td>172.1.1.1</td>
<td>1</td>
<td>01:51:40</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/0/7</td>
<td>10 7</td>
<td>10.0.0.68</td>
<td>8</td>
<td>172.1.1.1</td>
<td>1</td>
<td>01:51:05</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/1/0</td>
<td>19 8</td>
<td>10.0.0.68</td>
<td>9</td>
<td>172.1.1.1</td>
<td>1</td>
<td>01:50:55</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/1/1</td>
<td>20 9</td>
<td>10.0.0.68</td>
<td>10</td>
<td>172.1.1.1</td>
<td>1</td>
<td>01:50:43</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/1/2</td>
<td>21</td>
<td>10.0.0.68</td>
<td>11</td>
<td>172.1.1.1</td>
<td>1</td>
<td>01:46:37</td>
<td>00:00:00/5 min</td>
</tr>
<tr>
<td>0/1/3</td>
<td>22</td>
<td>10.0.0.68</td>
<td>12</td>
<td>172.1.1.1</td>
<td>1</td>
<td>01:46:28</td>
<td>00:00:00/5 min</td>
</tr>
</tbody>
</table>

### Configuring Raw Socket Transport on the Cisco ASR 903 Router

#### Sample Show Command Output

<table>
<thead>
<tr>
<th>Interface</th>
<th>Sessions</th>
<th>TCP In Bytes</th>
<th>TCP Out Bytes</th>
<th>TCP To TTY Frames</th>
<th>TTY To TCP Frames</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/0/0</td>
<td>3 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
<tr>
<td>0/0/1</td>
<td>4 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
<tr>
<td>0/0/2</td>
<td>5 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
<tr>
<td>0/0/3</td>
<td>6 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
<tr>
<td>0/0/4</td>
<td>7 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
<tr>
<td>0/0/5</td>
<td>8 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
<tr>
<td>0/0/6</td>
<td>9 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
<tr>
<td>0/0/7</td>
<td>10 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
<tr>
<td>0/1/0</td>
<td>19 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
<tr>
<td>0/1/1</td>
<td>20 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
<tr>
<td>0/1/2</td>
<td>21 1</td>
<td>9471</td>
<td>287847</td>
<td>351 351</td>
<td></td>
</tr>
</tbody>
</table>
Example for Raw Socket Global Routing Table Sample Configuration

**Server Configuration**

```plaintext
time line 

interface Serial0/1/0
no ip address
!
line 0/1/0
raw-socket tcp server 5000 10.1.1.1
raw-socket packet-timer 3
raw-socket tcp idle-timeout 5

interface Loopback0
ip address 10.1.1.1 255.255.255.255

router isis grid-ops
net 49.2222.0000.0000.0005.00
passive-interface Loopback0
```

**Client Configuration**

```plaintext
time line 

interface Serial0/1/0
no ip address
!
interface Serial0/1/1
no ip address
!
line 0/1/0
raw-socket tcp client 10.1.1.1 5000 2.2.2.2 9000
raw-socket packet-length 32
raw-socket tcp idle-timeout 5
!
line 0/1/1
raw-socket tcp client 10.1.1.1 5000 2.2.2.2 9001
raw-socket packet-length 32
raw-socket tcp idle-timeout 5

interface Loopback0
ip address 172.2.2.2 255.255.255.255

router isis grid-ops
net 49.2222.0000.0000.0005.00
passive-interface Loopback0
```

Example for Raw Socket MPLS VPN Sample Configuration

**Server Configuration**

```plaintext
time line 

interface Serial0/1/0
vrf forwarding scada
no ip address
!
line 0/1/0
raw-socket tcp server 5000 10.1.1.1
raw-socket packet-timer 3
```
Example for Raw Socket Global Routing Table Sample Configuration

```plaintext
raw-socket tcp idle-timeout 5

interface Loopback100
  vrf forwarding scada
  ip address 10.1.1.1 255.255.255.255

vrf definition scada
  rd 100:100
  
  address-family ipv4
    route-target export 1111:101
    route-target import 1111:101
  exit-address-family

router bgp 1111
  
  address-family vpnv4
  
  address-family ipv4 vrf scada
    redistribute connected
  exit-address-family

Client Configuration

interface Serial0/1/0
  vrf forwarding scada
  no ip address
  
  interface Serial0/1/1
    vrf forwarding scada
    no ip address
    
    line 0/1/0
      raw-socket tcp client 10.1.1.1 5000 2.2.2.2 9000
      raw-socket packet-length 32
      raw-socket tcp idle-timeout 5
    
    line 0/1/1
      raw-socket tcp client 10.1.1.1 5000 2.2.2.2 9001
      raw-socket packet-length 32
      raw-socket tcp idle-timeout 5

interface Loopback100
  vrf forwarding scada
  ip address 172.2.2.2 255.255.255.255

vrf definition scada
  rd 100:100
  
  address-family ipv4
    route-target export 1111:101
    route-target import 1111:101
  exit-address-family

router bgp 1111
  
  address-family vpnv4
  
  address-family ipv4 vrf scada
    redistribute connected
  exit-address-family
```

Time Division Multiplexing Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 900 Series)
Example for Raw Socket VRF Lite Sample Configuration

Server Configuration

```bash
interface Serial0/1/0
  vrf forwarding scada
  no ip address
!
line 0/1/0
  raw-socket tcp server 5000 10.1.1.1
  raw-socket packet-timer 3
  raw-socket tcp idle-timeout 5

interface GigabitEthernet0/0.10
  encapsulation dot1q 10
  vrf forwarding scada
  ip address 10.1.1.1 255.255.255.0

vrf definition scada
  rd 100:100
  address-family ipv4
    route-target export 100:101
    route-target import 100:101
  exit-address-family

router bgp 100
  address-family ipv4 vrf scada
    redistribute connected
  neighbor 10.1.1.2 remote-as 1111
  neighbor 10.1.1.2 activate
  exit-address-family
```

Client Configuration

```bash
interface Serial0/1/0
  vrf forwarding scada
  no ip address
!

interface Serial0/1/1
  vrf forwarding scada
  no ip address
!

line 0/1/0
  raw-socket tcp client 10.1.1.1 5000 20.1.1.1 9000
  raw-socket packet-length 32
  raw-socket tcp idle-timeout 5
!

line 0/1/1
  raw-socket tcp client 10.1.1.1 5000 20.1.1.1 9001
  raw-socket packet-length 32
  raw-socket tcp idle-timeout 5

interface GigabitEthernet0/0.10
  encapsulation dot1q 10
  vrf forwarding scada
  ip address 172.1.1.1 255.255.255.0

vrf definition scada
  rd 100:100
```
Related Documentation

For more information about the Cisco ASR 903 Router, refer to the following documents:

- Release Notes for the Cisco ASR 903 Router
- Regulatory Compliance and Safety Information for the Cisco ASR 903 Series Services Aggregation Router
- Cisco ASR 903 Series Aggregation Services Router Hardware Installation Guide
- Cisco ASR 903 Router Chassis Software Configuration Guide
CHAPTER 7

Transparent SONET or SDH over Packet (TSoP) Protocol

Note

Transparent SONET or SDH over Packet (TSoP) Protocol is not supported on the Cisco ASR 900 RSP3 module.

The Transparent SONET or SDH over Packet (TSoP) protocol converts SONET or SDH TDM traffic to a packet stream. Operators can now transport SONET or SDH traffic across a packet network by simply adding the TSoP Smart SFP to any router or packet switch. With TSoP the SONET or SDH signal is forwarded transparently, maintaining its embedded payload structure, protection protocols and synchronization. This simplifies the configuration and service turn-up of SONET or SDH connections across the packet network.

- Prerequisites for TSoP, on page 151
- Restrictions for TSoP, on page 151
- Information About TSoP Smart SFP, on page 152
- Configuring the Reference Clock, on page 153
- Configuration Examples for TSoP, on page 154
- Verification Examples, on page 156

Prerequisites for TSoP

- Single mode optical fiber must be used to connect TSoP Smart SFP with the OC-3 port.
- The TSoP smart SFP pseudowire endpoints must use the same configuration parameters.

Restrictions for TSoP

- The TSoP smart SFP payload size is not configurable. The byte size is fixed at 810 bytes.
- The router cannot be synced with the TSoP Smart SFP clock.
- Only untagged encapsulation is supported.
- CFM (connectivity fault management) is not supported.
Only QoS Default Experimental marking is supported.

TSOp can guarantee a sub 100 millisecond convergence time on SSO.

SSO is not supported on TSoP for STM-4 or OC-12 SFP due to hardware restriction.

TSOp is not supported on the 10G ports.

Information About TSoP Smart SFP

TSoP Smart SFP is a special type of optical transceiver which provides solution to transparently encapsulate SDH or SONET bit streams into packet format, suitable for pseudowire transport over an ethernet network. The TSoP pseudowires is manually configured or setup using PWE3 control protocol [RFC4447].

TSoP provides packetization, de-packetization, and clock recovery that translates the TDM bit stream to fixed size data blocks (810 octets), and vice verse.

TSoP follows the SAToP method described in [RFC4553] for pseudowire transport of E1/DS1, over a packet switched network. With TSoP, the entire OC-3 or STM-1 is encapsulated in a single circuit emulating pseudowire traffic, and is transported it to a single destination across the ethernet network.

The TSoP smart SFP is used on any of the front panel ports of the 8-port Gigabit Ethernet SFP Interface Module (8X1GE).

- The Smart SFP transceivers is compatible with the Small Form Factor Pluggable 20-pin Multi-Source Agreement (MSA).
- TSoP Smart SFP (PN: ONS-SC-155-TSOP) transports upto 155 Mbps, on a L1.1 (40km) optical data link.

Guidelines for TSoP Smart SFP

TSoP is compatible with the below SFPs supported on the OC-3 interface module. We recommend you use the specified attenuator:

- ONS-SI-155-I1—For 15km cable length, use 2 dB attenuator; short distance use 8 dB attenuator to avoid receiver overload.
- ONS-SI-155-L1—For 40km cable length, no attenuator; short distance use 10 dB attenuator to avoid receiver overload.
- ONS-SI-155-L2—For 40km cable length, use 2 dB attenuator; short distance use 10 dB attenuator to avoid receiver overload.

Multimode SFP is not supported with TSoP.

STM-4 TSoP is compatible with the below SFPs supported on the OC-12 interface module:
• ONS-SI-622-L2—For 40km cable length, use 2 dB attenuator; short distance use 10 dB attenuator to avoid receiver overload.

• ONS-SI-622-L1—For 40km cable length, no attenuator; short distance use 10 dB attenuator to avoid receiver overload.

• ONS-SI-622-I1—For 15km cable length, use 2 dB attenuator; short distance use 8 dB attenuator to avoid receiver overload.

---

**Note**

The OC-12 Smart SFP (PN: ONS-SC-622-TSOP) is *not* supported in Cisco IOS XE Release 3.14S.

---

**Note**

Effective Cisco IOS XE Release 3.18, STM-4 TSoP is supported on ASR 900 RSP2 Module.

---

## Configuring the Reference Clock

The reference clock for the TSoP is extracted from the network. You can extract the clock reference from either of the following:

- Ethernet physical interface
- Incoming TDM physical interface

---

**Note**

If TDM reference clock is configured, and you want to return to the Ethernet reference clock (default), use the `ssfpd tsop clock-source ethernet` command. Additionally, you can also use the `no ssfpd tsop clock-source` command to return the Ethernet reference clock (default).

---

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. ssfpd tsop clock-source {ethernet | tdm}
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: <code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------</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: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>interface type number</td>
<td>Specifies the Gigabit Ethernet interface for configuration and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# interface gigabitethernet 0/0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>ssfpd tsop clock-source {ethernet</td>
<td>tdm}</td>
</tr>
<tr>
<td>Example: Device(config)# ssfpd tsop clock-source ethernet</td>
<td></td>
</tr>
<tr>
<td>• ethernet — Specifies the ethernet interface as clock source. Default is ethernet.</td>
<td></td>
</tr>
<tr>
<td>• tdm — Specifies the TDM interface as clock source.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Exists configuration and enters privileged EXEC mode</td>
</tr>
<tr>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Examples for TSoP**

**Sample Configuration**

For configuring SONET or SDH controller as in the figure (network A and B), see Configuring Optical Interface Modules.

**Figure 10: TSoP in Packet Switched Network**

TSoP Smart SFP inserted in the PE’s, CE (SONET or SDH) can be configured as

• SDH or SONET framing for T1 and E1 mode.
• Serial interface in SDH or SONET mode. The scale for OC-3 IM is as supported—63 for E1 and 84 for T1 interfaces. The scale supported for OC-12 IM is 252 E1 and 336 T1 interfaces.

• Multilink interface with minimum of 1 member link and maximum of 16 member link.

• POS interface in SDH or SONET mode.

• ATM Layer 3 interfaces in SDH or SONET mode.

Note
ATM Layer 3 interface is not supported on CE for OC-12 IM.

• In OC-12 mode, if OC-12 IM is used on CE, only port 0 (ZERO) of the IM is used. Use the card-type command to operate the OC-12 IM.

For configuring the pseudowire using service instances, see Ethernet Virtual Connections Configuration on the Cisco ASR 903 Router.

Note
Only untagged encapsulation is supported.

• The following example shows a sample configuration on the CE:

```
controller SONET 0/2/3
framing sdh
clock source line
aug mapping au-3
!
au-3 1
overhead j1 length 64
mode c-11
tug-2 1 t1 1 channel-group 0 timeslots 1
```

• The following example shows a sample configuration of the Gigabit Ethernet interface with TSoP smart SFP installed:

```
interface GigabitEthernet0/0/0
no ip address
negotiation auto
no keepalive
service instance 1 ethernet
  encapsulation untagged
  xconnect 2.2.2.2 1 encapsulation mpls
```

Verification Examples

Verifying TSoP Smart SFP

• Use the `show inventory` command to display all TSoP Smart SFPs installed on the router.

Router# show inventory
NAME: "subslot 0/0 transceiver 7", DESCR: "TSoP OC-3/STM-1"
PID: ONS-SC-155-TSOP , VID: 01.0, SN: OES18100028

• Use the `show platform software ssfpd db` command to display all TSoP Smart SFPs recognized by the router.

Router# show platform software ssfpd db
=== Smart SFP info ===
dpidx: 14
mac : 00:19:3a:00:2f:18
port: 7
bay: 0
ssfp upgrade data store id: -1
ssfp is device upgrade safe: -1
upgrade percentage complete: 0
ssfp upgrade in progress: 0

• Use the `show platform software ssfpd db` command with slot, bay and port to display specific TSoP Smart SFPs recognized by the router.

Router# show platform software ssfpd slot 0 bay 0 port 7 ssfp-d
port 7 ssfp-db
dpidx: 14
mac : 00:19:3a:00:2f:18
port: 7
bay: 0
ssfp upgrade data store id: -1
ssfp device upgrade safe: -1
Upgrade percentage_complete: 0
ssfp upgrade in progress: 0

• Use the `show hw-module subslot` command to view information about TSoP Smart SFP.

Router# show hw-module subslot 0/0 transceiver 7 idprom
IDPROM for transceiver GigabitEthernet0/0/7:
Description = SFP or SFP+ optics (type 3)
Transceiver Type: = TSoP OC-3/STM-1 (291)
Product Identifier (PID) = ONS-SC-155-TSOP
Vendor Revision = 01.0
Serial Number (SN) = OES18100028
Vendor Name = CISCO-OES
Vendor OUI (IEEE company ID) = 00.19.3A (6458)
CLEI code = WOTRDBZBAA
Cisco part number = 10-2949-01
Device State = Enabled.
Date code (yy/mm/dd) = 14/03/07
Connector type = LC.
Encoding = 8B10B
NRZ
Nominal bitrate = OC3/STM1 (200 Mbits/s)

The following example shows the configuration of STM-4 TSoP:

NAME: “subslot 0/5 transceiver 2”, DESCR: “TSoP OC-12/STM-4”
PID: ONS-SC-622-TSOP, VID: 01.0, SN: OES17420029

Verifying Clock Source

• Use the `show platform software ssfpd` command to display the configured clock source. In the following example, `rtpClockSource` value for Ethernet clock source is displayed as 0. For TDM clock source the `rtpClockSource` value is displayed as 1.

Router# show platform software ssfpd slot 0 bay 0 port 7 encap-params
sdId: 14
channel: 0
iwfEncapOutputEnable: 1
ecid: 0
gAisTriggerActive: 0
gAisIncludeLosTrigger: 1
gAisIncludeLofTrigger: 1
insertRtpHeader: 1
rtpClockSource: 0
rtpFrequency: 0
rtpPayloadType: 0
rtpSrc: 0
Verifying Clock Source