



## **Time Division Multiplexing Configuration Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series)**

**First Published:** 2021-08-03

**Last Modified:** 2022-07-22

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

---

#### **Feature History 1**

---

### CHAPTER 2

#### **Configuring VCoP Smart SFP 3**

Features of VCoP Smart SFP 3

Benefits of VCoP Smart SFP 4

Prerequisites 4

Restrictions 5

Alarms on VCoP Smart SFP 6

Configuring VCoP Smart SFP 6

Configuring VCoP Smart SFP on OC-3 7

Enabling VCoP Smart SFP on OC-3 7

Configuring Framing for CEM Circuits for STS-1 on OC-3 7

Configuring CEM Circuits on VCoP for STS-3c on OC-3 8

Configuring Cross-Connect for STS-1 on OC-3 8

Configuring Cross-Connect for STS-3C on OC-3 8

Verifying VCoP Smart SFP Configuration for STS-1 on OC-3 8

Verifying VCoP Smart SFP Configuration for STS-3C on OC-3 10

Configuring VCoP Smart SFP on OC-12 11

Enabling VCoP Smart SFP on OC-12 11

Configuring Framing for CEM Circuits for STS-1 on OC-12 11

Configuring CEM Circuits on VCoP for STS-12C on OC-12 12

Configuring Cross-Connect for STS-1 on OC-12 12

Configuring Cross-Connect for STS-12C on OC-12 12

Verifying VCoP Smart SFP Configuration for STS-1 on OC-12 13

Verifying VCoP Smart SFP Configuration for STS-12C on OC-12 14

Configuring VCoP Smart SFP on T3 16

- Enabling VCoP Smart SFP on T3 16
- Configuring CEM Circuits on T3 VCoP Smart SFP 16
- Configuring Cablelength on T3 VCoP Smart SFP 16
- Configuring Cross-Connect on T3 VCoP Smart SFP 16
- Verifying VCoP Smart SFP Configuration on T3 16
- Performance Monitoring and Overhead Bytes 17
- Troubleshooting 20
  - Troubleshooting VCoP Smart SFP Configuration on OC-3 20
  - Troubleshooting VCoP Smart SFP Configuration on OC-12 21
  - Running Bit Error Rate Testing 22
    - Configuring BERT on OC-3/OC-12 VCoP Smart SFP 23
    - Configuring BERT on T3 VCoP Smart SFP 23
  - Loopback on VCoP Smart SFP 24
    - Configuring Loopback on VCoP STS1 Channel 24
    - Configuring Loopback on SONET Controller 26
    - Configuring Loopback on T3 VCoP Smart SFP 27
- Configuration Examples for VCoP Smart SFP 28
  - Example: VCoP Smart SFP Configuration on OC-3 28
  - Example: VCoP Smart SFP Configuration on OC-12 29
  - Example: VCoP Smart SFP Configuration on T3 30
- Associated Commands 31
- Additional References for VCoP Smart SFP 32

---

**CHAPTER 3**

**Configuring Pseudowire 33**

- Pseudowire Overview 33
  - Limitations 34
  - Circuit Emulation Overview 34
  - Structure-Agnostic TDM over Packet 35
  - Circuit Emulation Service over Packet-Switched Network 36
  - Asynchronous Transfer Mode over MPLS 38
  - Transportation of Service Using Ethernet over MPLS 39
- Limitations 39
- Configuring CEM 40
  - Configuration Guidelines and Restrictions 40

Configuring a CEM Group	40
Using CEM Classes	41
Configuring a Clear-Channel ATM Interface	44
Configuring CEM Parameters	44
Configuring Payload Size (Optional)	44
Setting the Dejitter Buffer Size	44
Setting an Idle Pattern (Optional)	44
Enabling Dummy Mode	44
Setting a Dummy Pattern	45
Shutting Down a CEM Channel	45
Configuring ATM	45
Configuring a Clear-Channel ATM Interface	45
Configuring ATM IMA	46
BGP PIC with TDM Configuration	49
Configuring Structure-Agnostic TDM over Packet (SAToP)	49
Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN)	50
Configuring a Clear-Channel ATM Pseudowire	52
Configuring an ATM over MPLS Pseudowire	53
Configuring the Controller	53
Configuring an IMA Interface	54
Configuring the ATM over MPLS Pseudowire Interface	55
Configuring 1-to-1 VCC Cell Transport Pseudowire	56
Configuring N-to-1 VCC Cell Transport Pseudowire	57
Configuring 1-to-1 VPC Cell Transport	57
Configuring ATM AAL5 SDU VCC Transport	59
Configuring a Port Mode Pseudowire	60
Optional Configurations	61
Configuring an Ethernet over MPLS Pseudowire	62
Configuring Pseudowire Redundancy	64
Pseudowire Redundancy with Uni-directional Active-Active	66
Restrictions	67
Configuring Pseudowire Redundancy Active-Active— Protocol Based	67
Configuring the Working Controller for MR-APS with Pseudowire Redundancy Active-Active	68
Configuring the Protect Controller for MR-APS with Pseudowire Redundancy Active-Active	68

Verifying the Interface Configuration	68
Configuration Examples	69
Example: CEM Configuration	69
Example: BGP PIC with TDM Configuration	70
Example: BGP PIC with TDM-PW Configuration	71
Example: ATM IMA Configuration	72
Example: ATM over MPLS	72
Cell Packing Configuration Examples	72
Cell Relay Configuration Examples	75
Example: Ethernet over MPLS	79

**CHAPTER 4****Configuring Multi Router Automatic Protection Switching 81**

Restrictions for MR-APS	81
Information About MR-APS	82
Configuring MR-APS with HSPW-ICRM on a CEM interface	84
Verifying MR-APS	88
Configuration Examples for MR-APS	95
Configuring MR-APS on a POS interface	97
Configuring working node for POS MR-APS	97
Configuring protect node for POS MR-APS	100
Verifying MR-APS on POS interface	102
Configuration Examples for MR-APS on POS interface	104

**CHAPTER 5****Hot Standby Pseudowire Support for ATM and TDM Access Circuits 107**

Prerequisites for Hot Standby Pseudowire Support for ATM and TDM Access Circuits	107
Restrictions for Hot Standby Pseudowire Support for ATM and TDM Access Circuits	108
Information About Hot Standby Pseudowire Support for ATM and TDM Access Circuits	108
How the Hot Standby Pseudowire Support for ATM and TDM Access Circuits Feature Works	108
Supported Transport Types	108
How to Configure Hot Standby Pseudowire Support for ATM and TDM Access Circuits	109
Configuring a Pseudowire for Static VPLS	109
Configuring Hot Standby Pseudowire Support for ATM and TDM Access Circuits	111
Verifying the Hot Standby Pseudowire Support for ATM and TDM Access Circuits Configuration	112
Configuration Examples for Hot Standby Pseudowire Support for ATM and TDM Access Circuits	114

Configuring Hot Standby Pseudowire Support for ATM and TDM Access Circuits on CEM Circuits Example	114
Additional References	118

**CHAPTER 6****PPP and Multilink PPP Configuration 121**

Limitations	121
PPP and Multilink PPP	122
Point-to-Point Protocol	122
CHAP or PPP Authentication	122
IP Address Pooling	123
Peer Address Allocation	123
Precedence Rules	124
MLP on Synchronous Serial Interfaces	124
How to Configure PPP	125
Enabling PPP Encapsulation	125
Enabling CHAP or PAP Authentication	126
Configuring IP Address Pooling	127
Global Default Address Pooling Mechanism	128
Defining DHCP as the Global Default Mechanism	128
Defining Local Address Pooling as the Global Default Mechanism	129
Controlling DHCP Network Discovery	130
Configuring IP Address Assignment	131
Disabling or Reenabling Peer Neighbor Routes	132
Configuring Multilink PPP	133
Configuring MLP on Synchronous Interfaces	133
Configuring a Multilink Group	134
Configuring PFC and ACFC	135
Changing the Default Endpoint Discriminator	138
Creating a Multilink Bundle	138
Assigning an Interface to a Multilink Bundle	139
Configuring PPP/MLP MRRU Negotiation Configuration on Multilink Groups	140
Monitoring and Maintaining PPP and MLP Interfaces	144

**CHAPTER 7****Transparent SONET or SDH over Packet (TSoP) Protocol 145**

Prerequisites for TSoP	146
Restrictions for TSoP	146
Information About TSoP Smart SFP	146
Guidelines for TSoP Smart SFP	147
Configuring the Reference Clock	148
Configuration Examples for TSoP	149
Verification Examples	150
Verifying TSoP Smart SFP	150
Verifying Clock Source	151

---

**CHAPTER 8**

<b>Configuring TPoP Smart SFP</b>	<b>153</b>
Features of TPoP Smart SFP	154
TPoP Prerequisites	155
Restrictions for TPoP Smart SFP	156
How to Configure TPoP Smart SFP	156
Enabling TPoP Smart SFP	156
Configuring CEM Circuits	157
Configuring Cable Length	157
Configuring Linecode	158
Configuring Dejitteer Buffer and Payload	159
Configuring BERT	159
Loopback on TPoP Smart SFP	160
Configuring Loopback on TPoP	160
Verifying Loopback at Controller Level	161
Performance Monitoring on TPoP	163
Configuring Clocking Recovery System for TPoP	164
Prerequisites for Clock Recovery	164
Configuring ACR	164
Configuring DCR	166
Verifying TPoP Smart SFP Configuration	168





# CHAPTER 1

## Feature History

The following table lists the new and modified features supported in the Time Division Multiplexing Configuration Guide in Cisco IOS XE 17 releases, on Cisco NCS 4206 and Cisco NCS 4216 routers.

Feature	Description
<b>Cisco IOS XE Cupertino 17.7.1</b>	
<a href="#">Framed SAToP support for T3 Smart TPoP pluggable</a>	<p>You can configure the following features for T3 in framed mode:</p> <ul style="list-style-type: none"> <li>• Loopback, framing, line code encoding, cable length, and jitter buffer</li> <li>• BERT</li> <li>• Performance monitoring counters and alarms</li> <li>• Alarm profiling</li> <li>• Clock recovery modes</li> </ul> <p>These features that are configured on framed and unframed T3 interfaces help you to monitor the traffic and troubleshoot errors or failures efficiently.</p>
<b>Cisco IOS XE Bengaluru 17.6.1</b>	
<a href="#">Support for T1 framed Smart TPoP pluggable</a>	<p>You can configure the following features for T1 in framed mode:</p> <ul style="list-style-type: none"> <li>• Loopback, framing, line code encoding, cable length, and jitter buffer</li> <li>• BERT</li> <li>• Performance monitoring counters and alarms</li> <li>• Alarm profiling</li> <li>• Clock recovery modes</li> </ul> <p>These features that are configured on framed and unframed T1 interfaces help you to monitor the traffic and troubleshoot errors or failures efficiently.</p>

Feature	Description
<a href="#">Support for E1 framed Smart TPOp pluggable</a>	<p>You can configure the following features for E1 in framed and unframed modes:</p> <ul style="list-style-type: none"><li>• Loopback, framing, line code encoding, cable length, and jitter buffer</li><li>• BERT</li><li>• Performance monitoring counters and alarms</li><li>• Alarm profiling</li><li>• Clock recovery modes</li></ul> <p>These features that are configured on framed and unframed E1 interfaces help you to monitor the traffic and troubleshoot errors or failures efficiently.</p>



## CHAPTER 2

# Configuring VCoP Smart SFP

The Virtual Container over Packet (VCoP) smart small form-factor pluggable (SFP) forwards the Plesiochronous Digital Hierarchy (PDH)/SONET signal transparently across the packet network. VCoP smart SFP is a special type of transceiver which encapsulates SONET frames on STS-1, STS-3c, or STS-12C , and T3 frames on STS-1 channels into a single circuit emulating pseudowire and transports it to a single destination over Packet Switched Network (PSN).



**Note** The VCoP smart SFP feature is supported only on Cisco NCS 4201 and Cisco NCS 4202 Series. With effect from Cisco IOS XE 16.5.1S Release, VCoP smart SFP supports T3 mode.

- [Features of VCoP Smart SFP, on page 3](#)
- [Benefits of VCoP Smart SFP, on page 4](#)
- [Prerequisites, on page 4](#)
- [Restrictions, on page 5](#)
- [Alarms on VCoP Smart SFP, on page 6](#)
- [Configuring VCoP Smart SFP, on page 6](#)
- [Performance Monitoring and Overhead Bytes, on page 17](#)
- [Troubleshooting, on page 20](#)
- [Configuration Examples for VCoP Smart SFP, on page 28](#)
- [Associated Commands, on page 31](#)
- [Additional References for VCoP Smart SFP, on page 32](#)

## Features of VCoP Smart SFP

VCoP smart SFP provides support for the following features:

- Supports configuration on Gigabit Ethernet(GE) and TenGigabit Ethernet(10GE) ports of the chassis.
- OC-3 or OC-12 mode supports 15-km Duplex over GE and 10GE.
- T3 mode supports 450ft over GE and 10GE.
- VCoP smart SFP on OCn mode supports 1310nm laser optics and is multi source agreement (MSA) compliant.
- Supports SONET CEP (IETF RFC 4842).

- For peer end, supports use of any SFP or interface module that supports CEP protocol.
- Supports pseudowire configuration.
- Supports Online Insertion and Removal (OIR).




---

**Note** If after configuring a VCoP smart SFP, you remove and reinsert the VCoP smart SFP, the configuration persists. But, if you insert a non-VCoP SFP, the configuration is removed.

---

- Supports packetization, de-packetization, and clock recovery.
- Supports Explicit Pointer Adjustment Relay (EPAR).
- Supports alarms and performance monitoring.
- Supports loopback and BERT.
- Supports the following jitter buffer values:
  - OC-3 - 8ms
  - OC-12 - 4ms
  - T3 - 8ms
- Both OCx and PDH are supported on Cisco NCS 4201 and NCS 4202 Routers.

## Benefits of VCoP Smart SFP

- Supports channelization upto STS1 channel
- Reduces network complexity

## Prerequisites

- The Multi-Protocol Label Switching (MPLS) and Interior Gateway Protocol (IGP) endpoints are up and running fine between the PE nodes.
- Ensure that SyncE is configured.
- Use the PTP Telecom profile, G.8265.1 for frequency synchronization, for CEM.
- VCoP smart SFP on OCn mode supports single-mode optical fiber cables.
- Port interface is set as default by using the **default int Gig 0/0/8** command before inserting VCoP smart SFP on GE or 10GE port.
- The GE or 10GE port interface is brought up using the **no shutdown** command.

- In cases where a non-VCoP SFP is to be inserted on any port from which any VCoP smart SFP is removed, then before inserting non-VCoP SFP, the VCoP smart SFP configuration is removed using the below commands:

- For OC-3

**no platform smart-sfp interface Gig x/y/z type oc3**

- For OC-12

**no platform smart-sfp interface Gig x/y/z type oc12**

- For T3

**no platform smart-sfp interface Gig x/y/z type ds3**

- For T1

**no platform smart-sfp interface Gig x/y/z type t1**



#### Note

- Replace GE with 10GE in the above commands to configure VCoP as 10GE port interface when inserted in a 10GE port.
- There is no need to remove **platform smart-sfp interface Gig/TenGig x/y/z type oc3/oc12/ds3** command for OC-3 and OC-12 modes and **platform smart-sfp interface Gig/TenGig x/y/z type T1** for T1 mode if you are replacing one VCoP smart SFP with the same or another VCoP smart SFP.
- Recovered clock configuration needs to be removed before applying the **no platform** command.

- To connect the CE nodes, VCoP smart SFP uses single mode fiber (SMF) over the LC optical interface for OCx mode and DIN 1.0/2.3 Coaxial connector cable for T3 mode.



#### Note

Recommended interfacing connector for the T3 VCoP SFP is Compel 1.0/2.3 Coaxial connector P/N 350.064.621.

## Restrictions

- The payload size is fixed to STS1 and is 783 bytes.
- VCoP smart SFP *does not* support Stateful Switchover (SSO).
- For QoS, VCoP smart SFP supports only the default MPLS experimental marking.
- At a time, OC-3/OC-12 supports BERT at any one path. T3 supports BERT only at one port.
- VCoP smart SFP *does not* support E3 mode.
- The chassis supports up to 12 VCoP smart SFPs.

- The T3 mode supports 1 CEP circuit and can sustain the traffic up to 45mbps.
- The Cisco NCS 4201 supports a maximum of 12 VCoP smart SFPs and only on GE ports of the top row.
- The Cisco NCS 4202 supports a maximum of eight VCoP smart SFPs and on all GE and 10GE ports.
- BERT on OCn VCoP is supported only at STS-1 path level. VCoP hardware does not support BERT at concatenated paths.
- BERT on DS3 VCoP is supported only in the Line direction.
- The VCoP CEM counters do not support L-bit and R-bit counters.

## Alarms on VCoP Smart SFP

VCoP smart SFP supports the following alarms on OC-3 or OC-12 mode:

- Loss of Signal (LOS)
- Loss of Frame (LOF)
- Alarm Indication Signal (MS-AIS, AU-AIS)
- Remote Defect Indication Line (RDI-L)
- Loss of Pointer (AU-LOP)
- Path Unequipped Indication Signal (PUNEQ)

VCoP smart SFP supports the following alarms on T3 mode:

- Loss of Signal (LOS)
- Loss of Frame (LOF)
- Alarm Indication Signal (MS-AIS, AU-AIS)
- Remote Alarm Indication (RAI)




---

**Note** Starting with Cisco IOS XE Amsterdam 17.3.1, Loss of Frame (LOF) is not supported on T3 mode.

---




---

**Note** In case of RDI-L (remote alarm), SONET controller does not go down as this is not a critical alarm.

---

## Configuring VCoP Smart SFP

### Before You Begin

Ensure MPLS and IGP are active between the PE nodes.



**Note** VCoP smart SFP supports the following valid CEP Pseudo Wire (PW) configurations:

Mode	CEP PWs
OC-3	3* STS-1 or 1* STS-3c
OC-12	Valid mix of STS-1, STS-3c or STS-12c
T3	1*STS-1

You can configure VCoP smart SFP on OC-3 or OC-12 mode.

1. Enable VCoP smart SFP using the **platform** command.
2. Configure controller for CEM circuits.
3. Configure xConnect for CEM circuit.

You can configure VCoP smart SFP on T3 mode.

1. Enable VCoP smart SFP using the **platform** command.
2. Configure controller for CEM circuits.
3. Configure cablelength.
4. Configure xConnect for CEM circuit.

## Configuring VCoP Smart SFP on OC-3

### Enabling VCoP Smart SFP on OC-3

You can enable VCoP smart SFP for STS1 and STS-3c channels on OC-3.

```
enable
configure terminal
platform smart-sfp interface GigabitEthernet 0/0/8 type OC3
exit
```

### Configuring Framing for CEM Circuits for STS-1 on OC-3

```
enable
configure terminal
controller SONET 0/0/8
framing sonet
sts-1 1
mode unframed
cem-group 20 cep
sts-1 2
mode unframed
cem-group 21 cep
sts-1 3
mode unframed
```

```
cem-group 22 cep
exit
```

## Configuring CEM Circuits on VCoP for STS-3c on OC-3

```
enable
configure terminal
controller SONET 0/0/10
framing sonet
sts-1 1-3 mode sts-3c
cem-group 0 cep
overhead c2 0
exit
```

## Configuring Cross-Connect for STS-1 on OC-3




---

**Note** Ensure that the VC number that is configured in **xconnect** command is the same on both PEs.

---

```
enable
configure terminal
interface CEM0/0/8
no ip address
cem 20
xconnect 2.2.2.2 3000 encapsulation mpls
cem 21
xconnect 2.2.2.2 3001 encapsulation mpls
cem 22
xconnect 2.2.2.2 3002 encapsulation mpls
exit
```

## Configuring Cross-Connect for STS-3C on OC-3

```
enable
configure terminal
interface GigabitEthernet0/0/10
no ip address
negotiation auto
interface CEM0/0/10
no ip address
cem 0
xconnect 2.2.2.2 1000 encapsulation mpls
exit
```

## Verifying VCoP Smart SFP Configuration for STS-1 on OC-3

Use the **show cem circuit** command to verify the VCoP smart SFP configuration.

```
Device# show cem circuit detail

CEM0/0/8, ID: 20, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, CEP state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 783
Framing: Unframed
CEM Defects Set
None
```



```

Signalling: No CAS
RTP: No RTP

Ingress Pkts:    24000          Dropped:          0
Egress Pkts:    24000          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              Severly Errored Sec: 0
Unavailable Sec: 0             Failure Counts:   0
Pkts Malformed: 0             JitterBuf Overrun: 0
    
```

```

CEM0/0/8, ID: 21, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, CEP state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 783
Framing: Unframed
CEM Defects Set
None
    
```

```

Signalling: No CAS
RTP: No RTP

Ingress Pkts:    24000          Dropped:          0
Egress Pkts:    24000          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              Severly Errored Sec: 0
Unavailable Sec: 0             Failure Counts:   0
Pkts Malformed: 0             JitterBuf Overrun: 0
    
```

```

CEM0/0/8, ID: 22, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, CEP state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 783
Framing: Unframed
CEM Defects Set
None
    
```

```

Signalling: No CAS
RTP: No RTP

Ingress Pkts:    24000          Dropped:          0
Egress Pkts:    24000          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              Severly Errored Sec: 0
Unavailable Sec: 0             Failure Counts:   0
Pkts Malformed: 0             JitterBuf Overrun: 0
    
```

```

Device# show cem circuit
CEM Int.      ID   Ctrlr   Admin   Circuit   AC
-----
    
```

```
CEM0/0/8      20  UP      UP      Active  UP
CEM0/0/8      21  UP      UP      Active  UP
CEM0/0/8      22  UP      UP      Active  UP
```

```
Device# show mpls 12 vc
```

Local intf	Local circuit	Dest address	VC ID	Status
CE0/0/8	CEM 20	2.2.2.2	3000	UP
CE0/0/8	CEM 21	2.2.2.2	3001	UP
CE0/0/8	CEM 22	2.2.2.2	3002	UP

## Verifying VCoP Smart SFP Configuration for STS-3C on OC-3

Use the **show controller** command to verify the VCoP smart SFP configuration.

```
Device#show controller sonet 0/0/10
SONET 0/0/10 is up.
  Hardware is 12xGE-4x10GE-FIXED

  Port configured rate: OC-3
  Applique type is Channelized Sonet/SDH
  Clock Source is Line
Medium info:
  Type: Sonet, Line Coding: NRZ,
SECTION:
  LOS = 0          LOF = 0          BIP(B1) = 0

SONET/SDH Section Tables
  INTERVAL      CV    ES    SES  SEFS
  15:58-16:11   0     0     0     0

LINE:
  AIS = 0          RDI = 0          REI = 0          BIP(B2) = 0
Active Defects: None
Detected Alarms: None
Asserted/Active Alarms: None
Alarm reporting enabled for: SLOS SLOF SF B1-TCA B2-TCA
BER thresholds: SF = 10e-3 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6
Rx: S1S0 = 40
   K1 = 00,   K2 = 00
   J0 = 01
   RX S1 = 00

Tx: S1S0 = 00
   K1 = 00,   K2 = 00
   J0 = 01

SONET/SDH Line Tables
  INTERVAL      CV    ES    SES  UAS
  15:58-16:11   0     0     0     0

High Order Path:

PATH 1:
  AIS = 0          RDI = 0          REI = 0          BIP(B3) = 0
  LOP = 0          PSE = 0          NSE = 0          NEWPTR = 0
  LOM = 0          PLM = 0          UNEQ = 0

Active Defects: None
Detected Alarms: None
```

```

Asserted/Active Alarms: None
Alarm reporting enabled for: PLOP LOM B3-TCA

TCA threshold: B3 = 10e-6
Rx: C2 = 00
Tx: C2 = 00

PATH TRACE BUFFER : UNSTABLE

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

SONET/SDH Path Tables
INTERVAL      CV      ES      SES      UAS
16:11-16:11   0       0       0       0

STS-1 1 - 3 mode sts-3c
  cep is configured: TRUE cem_id :0
Path 2:
  configured as member of a concatenated interface
Path 3:
  configured as member of a concatenated interface

```

## Configuring VCoP Smart SFP on OC-12

### Enabling VCoP Smart SFP on OC-12

You can enable VCoP smart SFP for STS-1 and STS-12C channels on OC-12.

```

enable
configure terminal
platform smart-sfp interface GigabitEthernet 0/0/8 type OC12
exit

```

### Configuring Framing for CEM Circuits for STS-1 on OC-12

```

enable
configure terminal
controller SONET 0/0/8
framing sonet
sts-1 1
mode unframed
cem-group 20 cep
sts-1 2
mode unframed
cem-group 21 cep
sts-1 3
mode unframed
cem-group 22 cep
sts-1 4
mode unframed
sts-1 5
mode unframed
sts-1 6
mode unframed
sts-1 7
mode unframed
sts-1 8

```

```

mode unframed
sts-1 9
mode unframed
sts-1 10
mode unframed
sts-1 11
mode unframed
sts-1 12
mode unframed
exit

```

## Configuring CEM Circuits on VCoP for STS-12C on OC-12

```

enable
configure terminal
controller SONET 0/0/8
framing sonet
sts-1 1-12 mode sts-12c
cem-group0 cep
overhead c2 2
exit

```

## Configuring Cross-Connect for STS-1 on OC-12

```

enable
configure terminal
interface CEM 0/0/8
no ip address
cem 20
xconnect 2.2.2.2 3000 encapsulation mpls
cem 21
xconnect 2.2.2.2 3001 encapsulation mpls
cem 22
xconnect 2.2.2.2 3002 encapsulation mpls
cem 23
cem 24
cem 25
cem 26
cem 27
cem 28
cem 29
cem 30
cem 31
exit

```

## Configuring Cross-Connect for STS-12C on OC-12

```

enable
configure terminal
interface GigabitEthernet 0/0/8
no ip address
negotiation auto
interface CEM 0/0/8
no ip address
cem 0
xconnect 2.2.2.2 2222 encapsulation mpls
exit

```

## Verifying VCoP Smart SFP Configuration for STS-1 on OC-12

Use the **show cem circuit** and **show mpls l2 vc** commands to verify the VCoP smart SFP configuration.

```
Device# show cem circuit detail
```

```
CEM0/0/8, ID: 20, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, CEP state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 783
Framing: Unframed
CEM Defects Set
None
```

```
Signalling: No CAS
RTP: No RTP
```

```
Ingress Pkts:    24000          Dropped:          0
Egress Pkts:    24000          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          Severly Errored Sec: 0
Unavailable Sec: 0          Failure Counts:   0
Pkts Malformed: 0          JitterBuf Overrun: 0
```

```
CEM0/0/8, ID: 21, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, CEP state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 783
Framing: Unframed
CEM Defects Set
None
```

```
Signalling: No CAS
RTP: No RTP
```

```
Ingress Pkts:    24000          Dropped:          0
Egress Pkts:    24000          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          Severly Errored Sec: 0
Unavailable Sec: 0          Failure Counts:   0
Pkts Malformed: 0          JitterBuf Overrun: 0
```

```
CEM0/0/8, ID: 22, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, CEP state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 783
Framing: Unframed
CEM Defects Set
None
```

```
Signalling: No CAS
```

```

RTP: No RTP

Ingress Pkts:   24000          Dropped:          0
Egress Pkts:   24000          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              Severly Errored Sec: 0
Unavailable Sec: 0             Failure Counts:   0
Pkts Malformed: 0             JitterBuf Overrun: 0

Device# show cem circuit
CEM Int.      ID   Ctrlr   Admin   Circuit   AC
-----
CEM0/0/8     20   UP      UP      Active    UP
CEM0/0/8     21   UP      UP      Active    UP
CEM0/0/8     22   UP      UP      Active    UP

Device# show mpls l2 vc

Local intf    Local circuit      Dest address      VC ID      Status
-----
CE0/0/8      CEM 20             2.2.2.2          3000       UP
CE0/0/8      CEM 21             2.2.2.2          3001       UP
CE0/0/8      CEM 22             2.2.2.2          3002       UP

```

## Verifying VCoP Smart SFP Configuration for STS-12C on OC-12

Use the **show controller** command to verify the VCoP smart SFP configuration.

```

Device# show controller sonet 0/0/8
SONET 0/0/8 is up.
  Hardware is 12xGE-4x10GE-FIXED

  Port configured rate: OC-3
  Applique type is Channelized Sonet/SDH
  Clock Source is Line
Medium info:
  Type: Sonet, Line Coding: NRZ,
SECTION:
  LOS = 0          LOF = 0          BIP(B1) = 0

SONET/SDH Section Tables
INTERVAL      CV   ES   SES  SEFS
16:01-16:09  0   0   0    0

LINE:
  AIS = 0          RDI = 0          REI = 0          BIP(B2) = 0
Active Defects: None
Detected Alarms: None
Asserted/Active Alarms: None
Alarm reporting enabled for: SLOS SLOF SF B1-TCA B2-TCA
BER thresholds: SF = 10e-3 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6
Rx: S1S0 = 40
   K1 = 00,   K2 = 00
   J0 = 01
   RX S1 = 00

Tx: S1S0 = 00
   K1 = 00,   K2 = 00

```

J0 = 01

SONET/SDH Line Tables

INTERVAL	CV	ES	SES	UAS
16:01-16:09	0	0	0	0

High Order Path:

PATH 1:

AIS = 0	RDI = 0	REI = 0	BIP(B3) = 0
LOP = 0	PSE = 0	NSE = 0	NEWPTR = 0
LOM = 0	PLM = 0	UNEQ = 0	

Active Defects: None  
 Detected Alarms: None  
 Asserted/Active Alarms: None  
 Alarm reporting enabled for: PLOP LOM B3-TCA

TCA threshold: B3 = 10e-6  
 Rx: C2 = 00  
 Tx: C2 = 02

PATH TRACE BUFFER : UNSTABLE

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

SONET/SDH Path Tables

INTERVAL	CV	ES	SES	UAS
16:09-16:09	0	0	0	0

STS-1 1 - 12 mode sts-12c  
 cep is configured: TRUE cem\_id :0  
 Path 2:  
 configured as member of a concatenated interface  
 Path 3:  
 configured as member of a concatenated interface  
 Path 4:  
 configured as member of a concatenated interface  
 Path 5:  
 configured as member of a concatenated interface  
 Path 6:  
 configured as member of a concatenated interface  
 Path 7:  
 configured as member of a concatenated interface  
 Path 8:  
 configured as member of a concatenated interface  
 Path 9:  
 configured as member of a concatenated interface  
 Path 10:  
 configured as member of a concatenated interface  
 Path 11:  
 configured as member of a concatenated interface  
 Path 12:  
 configured as member of a concatenated interface

## Configuring VCoP Smart SFP on T3

### Enabling VCoP Smart SFP on T3

```
enable
configure terminal
platform smart-sfp interface gigabitEthernet 0/0/10 type DS3
end
```

### Configuring CEM Circuits on T3 VCoP Smart SFP

```
enable
configure terminal
controller t3 0/0/10
cem-group 0 cep
end
```

### Configuring Cablelength on T3 VCoP Smart SFP

```
enable
configure terminal
controller t3 0/0/10
cablelength long
end
```



- 
- Note** The range of cablelength
- long - 224-450 ft
  - short - 0-224 ft
- 

### Configuring Cross-Connect on T3 VCoP Smart SFP

```
enable
configure terminal
interface cem 0/0/10
cem0
xconnect 10.10.10.10 204 encapsulation mpls
end
```

### Verifying VCoP Smart SFP Configuration on T3

Use the **show cem circuit** command to verify the VCoP smart SFP on T3 mode.

```
Device# show cem circuit interface cem0/0/10

CEM0/0/10, ID: 0, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, CEP state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 783
Framing: Unframed
```



```

CEM Defects Set
None

Signalling: No CAS
RTP: No RTP

Ingress Pkts:    64000          Dropped:          0
Egress Pkts:    64000          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              Severly Errored Sec: 0
Unavailable Sec: 0             Failure Counts:   0
Pkts Malformed: 0             JitterBuf Overrun: 0

```

Use the **show controllers** command to verify the controller configuration of VCoP smart SFP on T3 mode

```

Device# show controllers t3 0/0/10
T3 0/0/10 is up.
  Hardware is 12xGE-4x10GE-FIXED

  Applique type is Channelized T3/T1
  No alarms detected.
  Framing is Unframed, Line Code is B3ZS, Cablelength Short less than 225ft
  BER thresholds: SF = 10e-10 SD = 10e-10
  Clock Source is internal
  Equipment customer loopback
  Data in current interval (0 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation, 0 P-bit Err Secs
    0 P-bit Severly Err Secs, 0 Severly Err Framing Secs
    0 Unavailable Secs, 0 Line Errored Secs
    0 C-bit Errored Secs, 0 C-bit Severly Errored Secs
    0 Severly Errored Line Secs
    0 Far-End Errored Secs, 0 Far-End Severly Errored Secs
    0 CP-bit Far-end Unavailable Secs
    0 Near-end path failures, 0 Far-end path failures
    0 Far-end code violations, 0 FERF Defect Secs
    0 AIS Defect Secs, 0 LOS Defect Secs
    0 Bipolar Violations/Excessive Zero Errors
    0 Code Violations Path Errors, 14 B3 Errors

```

## Performance Monitoring and Overhead Bytes

The VCoP smart SFP supports the performance monitoring counter to maintain the path quality of the link.

You can view the statistics or error count that is generated on the VCoP smart SFP, if you have the configuration that is described:

```

enable
configure terminal
controller SONET 0/0/8
threshold b1-tca 8
threshold b2-tca 8
framing sonet
overhead j0 6
overhead s1s0 2
!

```

```

sts-1 1
overhead c2 2
threshold b3-ber_sd 8
threshold b3-ber_sf 8
overhead 1 message PATH_TRACE]
threshold b3-tca 8
mode unframed
cem-group 0 cep
!

```

The following parameters affect SONET configuration:

- Overhead - Sets the SONET overhead bytes in the frame header to a specific standards requirement, or to ensure interoperability with equipment from another vendors.
  - J0 - Sets the J0/C1 byte value in the SONET section overhead.




---

**Note** 1 byte, 16 bytes, and 64 bytes are the supported values for J0.

---

- J1 - Path Trace Byte
- C2- Path Signal label
- S1S0 - Sets the SS bits value of the H1 byte in the SONET line overhead
- Alarm Reporting - Enables reporting for all or selected alarms.
  - B1 - Section BIP Error (SF/SD)
  - B2 - Line BIP Error (SF/SD)
  - B3 (SF/SD) - STS Path BIP Error
  - sd-ber - Sets Signal Degrade BER threshold
  - sf-ber - Sets Signal failure BER threshold

The performance monitoring result is displayed using the **show controller** command. The following snippets are the performance monitoring details when the **show controller** command is executed.

```

Router# show controller sonet 0/0/8
SONET 0/0/8 is up.
  Hardware is 12xGE-4x10GE-FIXED

Port configured rate: OC3
Applique type is Channelized Sonet/SDH
Clock Source is Line
Medium info:
  Type: Sonet, Line Coding: NRZ,
SECTION:
  LOS = 0          LOF = 0          BIP (B1) = 0

SONET/SDH Section Tables
  INTERVAL    CV    ES    SES    SEFS
  12:25-12:25  0    0    0    0

LINE:
  AIS = 0          RDI = 0          REI = 0          BIP (B2) = 0

```

Active Defects: None  
 Detected Alarms: None  
 Asserted/Active Alarms: None  
 Alarm reporting enabled for: SLOS SLOF SF B1-TCA B2-TCA  
 BER thresholds: SF = 10e-3 SD = 10e-6  
 TCA thresholds: B1 = 10e-8 B2 = 10e-8  
 Rx: S1S0 = 40  
     K1 = 00, K2 = 00  
     J0 = 01  
     RX S1 = 00  
  
 Tx: S1S0 = 02  
     K1 = 00, K2 = 00  
     J0 = 06

SONET/SDH Line Tables  

INTERVAL	CV	ES	SES	UAS
12:25-12:25	0	0	0	0

High Order Path:

PATH 1:  

AIS = 0	RDI = 0	REI = 0	BIP(B3) = 0
LOP = 0	PSE = 0	NSE = 0	NEWPTR = 0
LOM = 0	PLM = 0	UNEQ = 0	

Active Defects: None  
 Detected Alarms: PAIS  
 Asserted/Active Alarms: PAIS  
 Alarm reporting enabled for: PLOP LOM B3-TCA

TCA threshold: B3 = 10e-6  
 Rx: C2 = 00  
 Tx: C2 = 02

PATH TRACE BUFFER : UNSTABLE

```

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
    
```

SONET/SDH Path Tables  

INTERVAL	CV	ES	SES	UAS
12:25-12:25	0	0	0	0

PATH 2:  

AIS = 0	RDI = 0	REI = 0	BIP(B3) = 0
LOP = 0	PSE = 0	NSE = 0	NEWPTR = 0
LOM = 0	PLM = 0	UNEQ = 0	

Active Defects: None  
 Detected Alarms: None  
 Asserted/Active Alarms: None  
 Alarm reporting enabled for: PLOP LOM B3-TCA

TCA threshold: B3 = 10e-6  
 Rx: C2 = 00  
 Tx: C2 = 02

PATH TRACE BUFFER : UNSTABLE

```

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
    
```

```

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

SONET/SDH Path Tables
INTERVAL      CV    ES    SES    UAS
12:25-12:25   0     0     0     0

PATH 3:
AIS = 0          RDI = 0          REI = 0          BIP(B3) = 0
LOP = 0          PSE = 0          NSE = 0          NEWPTR = 0
LOM = 0          PLM = 0          UNEQ = 0

Active Defects: None
Detected Alarms: None
Asserted/Active Alarms: None
Alarm reporting enabled for: PLOP LOM B3-TCA

TCA threshold:  B3 = 10e-6
Rx: C2 = 00
Tx: C2 = 02

PATH TRACE BUFFER : UNSTABLE

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

SONET/SDH Path Tables
INTERVAL      CV    ES    SES    UAS
12:25-12:25   0     0     0     0

STS-1 1 mode UNFRAMED
cep is configured: TRUE cem_id :0

STS-1 2 mode UNFRAMED
cep is configured: FALSE cem_id :0

STS-1 3 mode UNFRAMED
cep is configured: FALSE cem_id :0

```

## Troubleshooting

### Troubleshooting VCoP Smart SFP Configuration on OC-3

**Problem** Checking the MAC address of the VCoP smart SFP from database

**Possible Cause** None

**Solution** Use the **show platform software ssfpd** and **show inventory** commands to troubleshoot issues with the VCoP smart SFP configuration.

```

Device# show platform software ssfpd db

=== Redundancy role ===
RF role: Active

```

```

=== Smart SFP info ===
dpidx: 15
mac : 00:19:3a:00:79:58
port: 8
bay: 0
ssfp upgrade data store id: -1
ssfp is device upgrade safe: -1
upgrade percentage complete: 0
ssfp upgrade in progress: 0

fpga version of the VCoP
#####

Device# show platform software ssfpd slot 0 bay 0 port 8 version
sdid: 15
rma timestamp: 160209-09:21
rma version: 00060000
firmware: 03002400
ppactive: 00060000
ppstored: 00060000
--CN Information--
cnid: 0
mbid: 271
hwid: 1274
nabc: 0
sabc: 0
nmbc: 0
ReleaseType: OFFICIAL

Device# show inventory |
beg VCoPNAME: "subslot 0/0 transceiver 8", DESCR: "VCoP OC-3/OC-12" PID: ONS-SI-OC-VCOP
, VID: 01.0, SN: OEA19430007

```

## Troubleshooting VCoP Smart SFP Configuration on OC-12

**Problem** Checking the MAC address of the VCoP smart SFP from database

**Possible Cause** None

**Solution** Use the **show platform software ssfpd** and **show inventory** commands to troubleshoot issues with the VCoP smart SFP configuration.

```

Device#show platform software ssfpd db

=== Redundancy role ===
RF role: Active

=== Smart SFP info ===
dpidx: 15
mac : 00:19:3a:00:79:58
port: 8
bay: 0
ssfp upgrade data store id: -1
ssfp is device upgrade safe: -1
upgrade percentage complete: 0
ssfp upgrade in progress: 0

fpga version of the VCoP
#####

Device#show platform software ssfpd slot 0 bay 0 port 8 version
sdid: 15
rma timestamp: 160209-09:21

```

```

rma version: 00060000
firmware: 03002400
ppactive: 00060000
ppstored: 00060000
--CN Information--
cnid: 0
mbid: 271
hwid: 1274
nabc: 0
sabc: 0
nmbc: 0
ReleaseType: OFFICIAL

Device#show inventory
 | beg VCoPNAME: "subslot 0/0 transceiver 8", DESCR: "VCoP OC-3/OC-12"PID: ONS-SI-OC-VCOP
   , VID: 01.0, SN: OEA19430007

```

## Running Bit Error Rate Testing

Bit Error Rate Testing (BERT) is supported on VCoP smart SFP at the STS-1 path level. The OCn VCoP hardware does not support BERT at the concatenated level paths like STS-3c or STS-12c. The interfaces contain onboard BERT circuitry to send and detect a pattern.

When running a BERT test, your system expects to receive the same pattern that it is transmitting. To help ensure that the two common options are available:

- Use a loopback somewhere in the link or network.
- Configure remote testing equipment to transmit the same BERT test pattern at the same time.

VCoP smart SFP supports Pseudo Random Binary Sequence (PRBS) pattern.

Both the total number of error bits received and the total number of error bits received are available for analysis. You can select the testing period to be from 1 minute to 24 hours, and you can also retrieve the error statistics anytime during the BERT test.

BERT is supported in two directions:

- Line - supports BERT in TDM direction.
- System - supports BERT in PSN direction.




---

**Note** When the BERT is configured towards system direction, it internally loopbacks the TDM side locally.

---




---

**Note** DS3 VCoP supports BERT only in the Line direction.

---




---

**Note** Running BERT on DS3 VCoP triggers LOF alarm and it is cleared when BERT is over.

---

## Configuring BERT on OC-3/OC-12 VCoP Smart SFP

Follow these steps to configure BERT on VCoP STS-1 path for direction as line.

```
enable
configure terminal
controller SONET 0/0/9
sts-1 1
bert pattern pRBS interval 5 direction line
exit
```




---

**Note** To terminate a BERT test during the specified test period, use the **no bert** command.

---

You can view the results of a BERT test at the following times:

- After you terminate the test using the **no bert** command.
- After the test runs completely.
- Anytime during the test (in real time).

### Verifying BERT on OC3/OC12

Use the **show controller** command to verify the BERT configuration on VCoP smart SFP.

```
BERT test result (running)
Test Pattern : All 0's, Status : Not Sync, Sync Detected : 0
Interval : 5 minute(s), Time Remain : 4 minute(s)
Bit Errors (since BERT started): 0 bits,
Bits Received (since BERT started): 0 Kbits
Bit Errors (since last sync): 0 bits
Bits Received (since last sync): 0 Kbits
Direction : Line
```

## Configuring BERT on T3 VCoP Smart SFP

Follow these steps to configure BERT on T3 VCoP smart SFP.

```
enable
configure terminal
controller t3 0/0/10
bert pattern pRBS interval 2
exit
```




---

**Note** To terminate a BERT test during the specified test period, use the **no bert** command.

---

You can view the results of a BERT test at the following times:

- After you terminate the test using the **no bert** command.
- After the test runs completely.
- Anytime during the test (in real time).

## Verifying BERT on T3 VCoP Smart SFP

Use the **show controller** command to verify the BERT configuration on T3 VCoP smart SFP.

```
Device# show controllers t3 0/0/10 | sec BERT
BERT test result (running)
  Test Pattern : 2^15, Status : Sync, Sync Detected : 5
  DSX3 BERT direction : Line
  Interval : 2 minute(s), Time Remain : 1 minute(s)
  Bit Errors (since BERT started): 0 bits,
  Bits Received (since BERT started): 0 Kbits
  Bit Errors (since last sync): 0 bits
  Bits Received (since last sync): 0 Kbits
```




---

**Note** BERT sync status gets updated once in every 5 seconds during the test interval on OCn and DS3 VCoP SSFPs.

The Sync detected status is incremented only if there is a change in BERT Sync states — NOT SYNC to SYNC.

---




---

**Note** BERT Statistics (Bit errors and Bits received) do not increment and are always shown as 0, on OCn and DS3 VCoP SSFPs.

---

## Loopback on VCoP Smart SFP

VCoP smart SFP supports two types of loopback configurations:

- Local loopback - In local loopback, the transmitting signal is looped back to the receiver signal.
- Network loopback - In network loopback, the receiving signal is looped back to the transmitting signal.

You can configure loopback on VCoP smart SFP at two levels:

- Controller level
- Path Level

## Configuring Loopback on VCoP STS1 Channel

### Configuring Network Loopback

Follow these steps to configure network loopback on VCoP STS1 channel.

```
enable
configure terminal
controller SONET 0/0/8
sts-1 1
loopback network
exit
```



## Configuring Local Loopback

Follow these steps to configure local loopback on VCoP STS1 channel.

```
enable
configure terminal
controller SONET 0/0/8
sts-1 1
loopback local
exit
```

## Verifying Loopback at Path Level

Use the **show run controller sonet 0/0/8** command to verify the configuration with loopback on VCoP smart SFP.

```
Controller SONET 0/0/11
no TU-AIS
threshold sf-ber 3
threshold b1-tca 8
threshold b2-tca 8
framing sonet
overhead j0 6
overhead sls0 2
!
sts-1 1 - 12 mode sts-12c
cem-group 0 cep
loopback local
overhead c2 2
threshold b3-ber_sd 8
threshold b3-ber_sf 8
overhead j1 message PATH_T
threshold b3-tca 8
```

Use the **show controller sonet 0/0/8** command to verify the path level local loopback configuration on VCoP smart SFP.

```
SONET 0/0/8 is up.
  Hardware is A900-IMA8S

  Port configured rate: OC3
  Applique type is Channelized Sonet/SDH
  ....
  .....
  .....
SONET/SDH Path Tables
  INTERVAL      CV    ES    SES    UAS
  02:32-02:32   0     0     0     0

STS-1 1 mode UNFRAMED
  cep is configured: TRUE cem_id :10
  Configured Loopback :  Locally Looped
```

Use the **show controller sonet 0/0/8** command to verify the path level network loopback configuration on VCoP smart SFP.

```
SONET 0/0/8 is up.
  Hardware is A900-IMA8S

  Port configured rate: OC3
  Applique type is Channelized Sonet/SDH
```

```

Clock Source is Line
....
.....
SONET/SDH Path Tables
  INTERVAL      CV    ES    SES    UAS
  02:35-02:35   0    0    0    0

STS-1 1 mode UNFRAMED
  cep is configured: TRUE cem_id :10
  Configured Loopback : Network Looped

```

## Configuring Loopback on SONET Controller

### Configuring Network Loopback

Follow these steps to configure network loopback on SONET controller.

```

enable
configure terminal
controller SONET 0/0/8
loopback network
exit

```

### Configuring Local Loopback

Follow these steps to configure local loopback on SONET controller.

```

enable
configure terminal
controller SONET 0/0/8
loopback local
exit

```

### Verifying Loopback at Controller Level

Use the **show controller sonet 0/0/8** command to verify the controller level local loopback configuration on VCoP smart SFP.

```

SONET 0/0/8 is up.(Configured for Locally Looped)
  Hardware is A900-IMA8S

  Port configured rate: OC3
  Applique type is Channelized Sonet/SDH
  ....
  .....

```

Use the **show controller sonet 0/0/8** command to verify the BERT configuration on VCoP Smart SFP.

```

SONET 0/0/8 is up.(Configured for Network Looped)
  Hardware is A900-IMA8S

  Port configured rate: OC3
  Applique type is Channelized Sonet/SDH
  ....
  .....

```

## Configuring Loopback on T3 VCoP Smart SFP

Follow these steps to configure local loopback on T3 VCoP smart SFP.

```
enable
configure terminal
controller t3 0/0/10
loopback local
end
```

Follow these steps to configure network loopback on T3 VCoP smart SFP.

```
enable
configure terminal
controller t3 0/0/10
loopback network
end
```




---

**Note** To remove loopback, use the **no loopback** command.

---

## Verifying Loopback on T3 VCoP Smart SFP

Use the **show controllers** command to verify the loopback local configuration on the T3 VCoP smart SFP.

```
Device# show controllers t3 0/0/10
T3 0/0/10 is up. (Configured for Locally Looped)
Hardware is 12xGE-4x10GE-FIXED

Applique type is Channelized T3/T1
No alarms detected.
Framing is Unframed, Line Code is B3ZS, Cablelength Short less than 225ft
BER thresholds: SF = 10e-10 SD = 10e-10
Clock Source is internal
Equipment customer loopback
Data in current interval (0 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  0 Severely Errored Line Secs
  0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
  0 CP-bit Far-end Unavailable Secs
  0 Near-end path failures, 0 Far-end path failures
  0 Far-end code violations, 0 FERF Defect Secs
  0 AIS Defect Secs, 0 LOS Defect Secs
  0 Bipolar Violations/Excessive Zero Errors
  0 Code Violations Path Errors, 14 B3 Errors
```

Use the **show controllers** command to verify the loopback network configuration on the T3 VCoP smart SFP.

```
Device# show controllers t3 0/0/10
T3 0/0/10 is up. (Configured for Looped toward the Network)
Hardware is 12xGE-4x10GE-FIXED

Applique type is Channelized T3/T1
No alarms detected.
```

```

Framing is Unframed, Line Code is B3ZS, Cablelength Short less than 225ft
BER thresholds: SF = 10e-10 SD = 10e-10
Clock Source is line
Equipment customer loopback
Data in current interval (0 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  0 Severely Errored Line Secs
  0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
  0 CP-bit Far-end Unavailable Secs
  0 Near-end path failures, 0 Far-end path failures
  0 Far-end code violations, 0 FERF Defect Secs
  0 AIS Defect Secs, 0 LOS Defect Secs
  0 Bipolar Violations/Excessive Zero Errors
  0 Code Violations Path Errors, 14 B3 Errors

```

## Configuration Examples for VCoP Smart SFP

### Example: VCoP Smart SFP Configuration on OC-3

```

Enabling the VCoP SSFP.
#####
platform smart-sfp interface GigabitEthernet0/0/8 type OC3

configuring the sonet controller.
=====
controller SONET 0/0/8
  framing sonet
  !
  sts-1 1
    mode unframed
    cem-group 20 cep
  !
  sts-1 2
    mode unframed
    cem-group 21 cep
  !
  sts-1 3
    mode unframed
    cem-group 22 cep
  !
  configuring the cem interface
  #####
interface CEM0/0/8
  no ip address
  cem 20
    xconnect 2.2.2.2 3000 encapsulation mpls
  !
  cem 21
    xconnect 2.2.2.2 3001 encapsulation mpls
  !
  cem 22
    xconnect 2.2.2.2 3002 encapsulation mpls
  !

```

## Example: VCoP Smart SFP Configuration on OC-12

```
Enabling the VCoP SSFP.
#####
platform smart-sfp interface GigabitEthernet0/0/8 type OC12

configuring the sonet controller.
=====
controller SONET 0/0/8
 framing sonet
 !
 sts-1 1
  mode unframed
  cem-group 20 cep
 !
 sts-1 2
  mode unframed
  cem-group 21 cep
 !
 sts-1 3
  mode unframed
  cem-group 22 cep
 !
 sts-1 4
  mode unframed

 !
 sts-1 5
  mode unframed

 !
 sts-1 6
  mode unframed

 !
 sts-1 7
  mode unframed

 !
 sts-1 8
  mode unframed

 !
 sts-1 9
  mode unframed

 !
 sts-1 10
  mode unframed

 !
 sts-1 11
  mode unframed

 !
 sts-1 12
  mode unframed

 !

configuring the cem interface
#####
interface CEM0/0/8
```

```

no ip address
cem 20
  xconnect 2.2.2.2 3000 encapsulation mpls
  !
cem 21
  xconnect 2.2.2.2 3001 encapsulation mpls
  !
cem 22
  xconnect 2.2.2.2 3002 encapsulation mpls
  !
cem 23
  !
cem 24

!
cem 25

!
cem 26

!
cem 27

!
cem 28

!
cem 29

!
cem 30
  !
cem 31

!
!
```

## Example: VCoP Smart SFP Configuration on T3

```

Enabling the VCoP SSFP.
#####
platform smart-sfp interface gigabitEthernet 0/0/10 type DS3

%DSX-4-ALARM: T3 0/0/10 DS3_RX_RAI: CLEARED
%CONTROLLER-5-UPDOWN: Controller T3 0/0/10, changed state to up
%LINK-3-UPDOWN: Interface T3 0/0/10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface T3 0/0/10, changed state to up

configuring the t3 controller.
=====
controller t3 0/0/10
cem-group 0 cep

%LINEPROTO-5-UPDOWN: Line protocol on Interface CEM0/0/10, changed state to up
%LINK-3-UPDOWN: Interface CEM0/0/10, changed state to up

cnfiguring the cem interface
#####
interface cem0/0/10
  cem 0
```

```
xconnect 2.2.2.2 101 encapsulation mpls
!
```

## Associated Commands

The commands used to configure VCoP Smart SFP.

Commands	URL
<b>platform smart-sfp</b>	<a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp2283539401">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp2283539401</a>
<b>controller sonet</b>	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp2020468554">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp2020468554</a>
<b>framing sonet</b>	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp6807068490">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp6807068490</a>
<b>controller t3</b>	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp1921350260">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp1921350260</a>
<b>sts-1</b>	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s6.html#wp2423232697">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s6.html#wp2423232697</a>
<b>cem-group</b>	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2440628600">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2440628600</a>
<b>xconnect</b>	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-t2.html#wp8578094790">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-t2.html#wp8578094790</a>
<b>overhead</b>	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp1973678817">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp1973678817</a>
<b>bert pattern</b>	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-a1.html#wp3620978929">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-a1.html#wp3620978929</a>
<b>show cem circuit</b>	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp7026926390">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp7026926390</a>
<b>loopback</b>	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-l1.html#wp1033903426">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-l1.html#wp1033903426</a>

Commands	URL
show controller sonet	<a href="http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s3.html#wp1341372847">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s3.html#wp1341372847</a>

## Additional References for VCoP Smart SFP

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>

### Standards and RFCs

Standard/RFC	Title
IETF RFC: 4842	<i>Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) - Circuit Emulation over Packet (CEP)</i>

### MIBs

MIB	MIBs Link
• <b>CCOMB</b>	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>

### Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>





## CHAPTER 3

# Configuring Pseudowire

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

- [Pseudowire Overview, on page 33](#)
- [Limitations, on page 39](#)
- [Configuring CEM, on page 40](#)
- [Configuring ATM, on page 45](#)
- [Configuring Structure-Agnostic TDM over Packet \(SAToP\), on page 49](#)
- [Configuring Circuit Emulation Service over Packet-Switched Network \(CESoPSN\), on page 50](#)
- [Configuring a Clear-Channel ATM Pseudowire, on page 52](#)
- [Configuring an ATM over MPLS Pseudowire, on page 53](#)
- [Configuring an Ethernet over MPLS Pseudowire, on page 62](#)
- [Configuring Pseudowire Redundancy, on page 64](#)
- [Pseudowire Redundancy with Uni-directional Active-Active , on page 66](#)
- [Restrictions , on page 67](#)
- [Configuring Pseudowire Redundancy Active-Active— Protocol Based, on page 67](#)
- [Configuring the Working Controller for MR-APS with Pseudowire Redundancy Active-Active, on page 68](#)
- [Configuring the Protect Controller for MR-APS with Pseudowire Redundancy Active-Active, on page 68](#)
- [Verifying the Interface Configuration, on page 68](#)
- [Configuration Examples, on page 69](#)

## 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 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 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 71](#).
- 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.

The following restrictions are applicable only if the BFD echo mode is enabled on the Ethernet interface carrying CEM or TDM traffic:

- When the TDM interface module is present in anyone of the slot—0, 1, or 2, then the corresponding Ethernet interface module carrying the CEM traffic should also be present in one of these slots.
- When the TDM interface module is present in anyone of the slot—3, 4, or 5, then the corresponding Ethernet interface module carrying the CEM traffic should also be present in one of these slots.

## 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



---

**Note** CEM pseudowire with local loopback at the CEM sides of PEs results in propagating AIS and L-bit alarms.

The L-bit packets are dropped for the following interface module:

- NCS4200-8E1T1-CE
- 

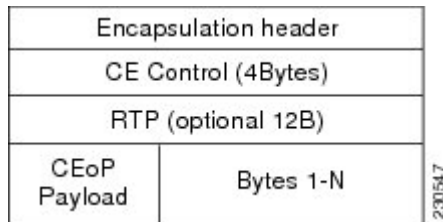
## Structure-Agnostic TDM over Packet

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 36](#) shows the frame format in Unstructured SAToP mode.

Figure 1: Unstructured SAToP Mode Frame Format



[#unique\\_54 unique\\_54\\_Connect\\_42\\_tab\\_1729930](#) shows the payload and jitter limits for the T1 lines in the SAToP frame format.

Table 1: SAToP T1 Frame: Payload and Jitter Limits

Maximum Payload	Maximum Jitter	Minimum Jitter	Minimum Payload	Maximum Jitter	Minimum Jitter
960	320	10	192	64	2

[#unique\\_54 unique\\_54\\_Connect\\_42\\_tab\\_1729963](#) shows the payload and jitter limits for the E1 lines in the SAToP frame format.

Table 2: SAToP E1 Frame: Payload and Jitter Limits

Maximum Payload	Maximum Jitter	Minimum Jitter	Minimum Payload	Maximum Jitter	Minimum Jitter
1280	320	10	256	64	2

For instructions on how to configure SAToP, see [Configuring Structure-Agnostic TDM over Packet \(SAToP\)](#), on page 49.

## 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 37](#) shows the frame format in CESoPSN mode.







**Note** This release does not support AToM N-to-1 Cell Mode or 1-to-1 Cell Mode.

For more information about how to configure AToM, see [Configuring an ATM over MPLS Pseudowire](#), on page 53.

## 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 62.

## Limitations

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-overr 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 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 71.
- 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.

The following restrictions are applicable only if the BFD echo mode is enabled on the Ethernet interface carrying CEM or TDM traffic:

- When the TDM interface module is present in anyone of the slot—0, 1, or 2, then the corresponding Ethernet interface module carrying the CEM traffic should also be present in one of these slots.
- When the TDM interface module is present in anyone of the slot—3, 4, or 5, then the corresponding Ethernet interface module carrying the CEM traffic should also be present in one of these slots.

## 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 49 and [Configuring Circuit Emulation Service over Packet-Switched Network \(CESoPSN\)](#), on page 50 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.

### Procedure

---

**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**    **controller {t1 | e1} slot/subslot/port****Example:**

```
Router(config)# controller t1 1/0
```

Enters controller configuration mode.

- Use the slot and port arguments to specify the slot number and port number to be configured.

**Note**        The slot number is always 0.

**Step 4**    **cem-group group-number {unframed | timeslots timeslot}****Example:**

```
Router(config-controller)# cem-group 6 timeslots 1-4,9,10
```

Creates a circuit emulation channel from one or more time slots of a T1 or E1 line.

- The **group-number** keyword identifies the channel number to be used for this channel. For T1 ports, the range is 0 to 23. For E1 ports, the range is 0 to 30.
- Use the **unframed** keyword to specify that a single CEM channel is being created including all time slots and the framing structure of the line.
- Use the **timeslots** keyword and the *timeslot* argument to specify 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.

**Step 5**    **end****Example:**

```
Router(config-controller)# end
```

Exits controller configuration mode and returns to privileged EXEC mode.

## 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 class:




---

**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.

---

### Procedure

---

**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**    **class cem *cem-class***

**Example:**

```
Router(config)# class cem mycemclass
```

Creates a new CEM class

**Step 4**    **payload-size *size* / de jitter-buffer *buffer-size* / idle-pattern *pattern***

**Example:**

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

**Example:**

```
Router(config-cem-class)# de jitter-buffer 10
```

**Example:**

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

Enter the configuration commands common to the CEM class. This example specifies a sample rate, payload size, de jitter buffer, and idle pattern.

**Step 5**    **exit**

**Example:**

```
Router(config-cem-class)# exit
```

Returns to the config prompt.

**Step 6** **interface cem slot/subslot****Example:****Example:**

```
Router(config)# interface cem 0/0
```

**Example:**

```
Router(config-if)# no ip address
```

**Example:**

```
Router(config-if)# cem 0
```

**Example:**

```
Router(config-if-cem)# cem class mycemclass
```

**Example:**

```
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
```

**Example:**

Configure the CEM interface that you want to use for the new CEM class.

**Note** The use of the **xconnect** command can vary depending on the type of pseudowire you are configuring.

**Step 7** **exit****Example:**

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

**Example:**

Exits the CEM interface.

**Step 8** **exit****Example:**

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

**Example:**

Exits configuration mode.

---

## 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 `pay-load 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:

```
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:

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



**Note** The dummy-pattern command is *not* supported on the following interface modules:

- 48-Port T3/E3 CEM interface module
- 48-Port T1/E1 CEM interface module
- 1-port OC-192 Interface module or 8-port Low Rate interface module

## 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:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>controller {t1} slot/subslot/port</b> <b>Example:</b> <pre>Router(config)# controller t1 0/3/0</pre>	Selects the T1 controller for the port you are configuring (where <i>slot/subslot</i> identifies the location and <i>/port</i> identifies the port).
<b>Step 4</b>	<b>atm</b> <b>Example:</b> <pre>Router(config-controller)# atm</pre>	Configures the port (interface) for clear-channel ATM. The router creates an ATM interface whose format is <i>atm/slot/subslot/port</i> . <b>Note</b> The slot number is always 0.
<b>Step 5</b>	<b>end</b> <b>Example:</b> <pre>Router(config-controller)# end</pre>	Exits configuration mode.

**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 33](#)

## 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.



**Note** ATM IMA is used as an element in configuring ATM over MPLS pseudowires. For more information about configuring pseudowires, see [Configuring Pseudowire, on page 33](#)



**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.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>card type {t1   e1} slot [bay]</b> <b>Example:</b> Router(config)# <b>card type e1 0 0</b>	Specifies the slot and port number of the E1 or T1 interface.
<b>Step 4</b>	<b>controller {t1   e1} slot/subslot/port</b> <b>Example:</b> Router(config)# <b>controller e1 0/0/4</b> <b>Example:</b>	Specifies the controller interface on which you want to enable IMA.
<b>Step 5</b>	<b>clock source internal</b> <b>Example:</b> Router(config-controller)# <b>clock source internal</b> <b>Example:</b>	Sets the clock source to internal.
<b>Step 6</b>	<b>ima group group-number</b> <b>Example:</b> Router(config-controller)# ima-group 0 scrambling-payload <b>Example:</b>	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.  <b>Note</b> This command automatically creates an ATM0/IMAx interface.  To add another member link, repeat <a href="#">Step 3</a> to <a href="#">Step 6</a> .
<b>Step 7</b>	<b>exit</b> <b>Example:</b>	Exits the controller interface.

	Command or Action	Purpose
	Router(config-controller)# <b>exit</b> <b>Example:</b>	
<b>Step 8</b>	<b>interface ATMslot/subslot/IMA group-number</b> <b>Example:</b> Router(config-if)# interface atm0/1/ima0	Specify the slot location and port of IMA interface group. <ul style="list-style-type: none"> <li>• <i>slot</i>—The location of the ATM IMA interface module.</li> <li>• <i>group-number</i>—The IMA group.</li> </ul> The example specifies the slot number as 0 and the group number as 0. <p><b>Note</b> To explicitly configure the IMA group ID for the IMA interface, use the optional <b>ima group-id</b> 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.</p>
<b>Step 9</b>	<b>no ip address</b> <b>Example:</b> Router(config-if)# no ip address	Disables the IP address configuration for the physical layer interface.
<b>Step 10</b>	<b>atm bandwidth dynamic</b> <b>Example:</b> Router(config-if)# atm bandwidth dynamic	Specifies the ATM bandwidth as dynamic.
<b>Step 11</b>	<b>no atm ilmi-keepalive</b> <b>Example:</b> Router(config-if)# no atm ilmi-keepalive	Disables the Interim Local Management Interface (ILMI) keepalive parameters. <p>ILMI is not supported on the router starting with Cisco IOS XE Release 3.15S.</p>
<b>Step 12</b>	<b>exit</b> <b>Example:</b>	Exits configuration mode.



	Command or Action	Purpose
	Router(config)# exit	

**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 40](#).

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 70](#).

## Configuring Structure-Agnostic TDM over Packet (SAToP)

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

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>controller [t1 e1] slot/subslot</b> <b>Example:</b> Router(config-controller)# controller t1 0/4	Configures the T1 or E1 interface.
<b>Step 4</b>	<b>cem-group group-number {unframed   timeslots timeslot}</b> <b>Example:</b> Router(config-if)# cem-group 4 unframed	Assigns channels on the T1 or E1 circuit to the CEM channel. This example uses the <b>unframed</b> parameter to assign all the T1 timeslots to the CEM channel.
<b>Step 5</b>	<b>interface cem slot/subslot</b> <b>Example:</b>	Defines a CEM group.

	Command or Action	Purpose
	<pre>Router(config)# interface CEM 0/4</pre> <p><b>Example:</b></p> <pre>Router(config-if)# no ip address</pre> <p><b>Example:</b></p> <pre>Router(config-if)# cem 4</pre>	
<b>Step 6</b>	<p><b>xconnect</b> <i>ip_address</i> <b>encapsulation mpls</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# xconnect 10.10.2.204 encapsulation mpls</pre>	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.
<b>Step 7</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config)# exit</pre>	Exits configuration mode.

**What to do next**

**Note** 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**.

## Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN)

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>controller</b> [e1   t1] <i>slot/subslot</i> <b>Example:</b> <pre>Router(config)# controller e1 0/0</pre> <b>Example:</b>	Enters configuration mode for the E1 or T1 controller.
<b>Step 4</b>	<b>cem-group</b> <i>group-number timeslots timeslots</i> <b>Example:</b> <pre>Router(config-controller)# cem-group 5 timeslots 1-24</pre>	Assigns channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the <b>timeslots</b> parameter to assign specific timeslots to the CEM channel.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> <pre>Router(config-controller)# exit</pre>	Exits controller configuration.
<b>Step 6</b>	<b>interface cem</b> <i>slot/subslot</i> <b>Example:</b> <pre>Router(config)# interface CEM0/5</pre> <b>Example:</b> <pre>Router(config-if-cem)# cem 5</pre> <b>Example:</b>	Defines a CEM channel.
<b>Step 7</b>	<b>xconnect</b> <i>ip_address encapsulation mpls</i> <b>Example:</b> <pre>Router(config-if)# xconnect 10.10.2.204 encapsulation mpls</pre>	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.
<b>Step 8</b>	<b>exit</b> <b>Example:</b> <pre>Router(config-if-cem)# exit</pre>	Exits the CEM interface.
<b>Step 9</b>	<b>exit</b> <b>Example:</b> <pre>Router(config)# exit</pre>	Exits configuration mode.

## Configuring a Clear-Channel ATM Pseudowire

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

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>controller {t1} slot/subslot/port</b> <b>Example:</b> <pre>Router(config)# controller t1 0/4</pre>	Selects the T1 controller for the port you are configuring. <b>Note</b> The slot number is always 0.
<b>Step 2</b>	<b>atm</b> <b>Example:</b> <pre>Router(config-controller)# atm</pre>	Configures the port (interface) for clear-channel ATM. The router creates an ATM interface whose format is <code>atm/slot/subslot/port</code> . <b>Note</b> The slot number is always 0.
<b>Step 3</b>	<b>exit</b> <b>Example:</b> <pre>Router(config-controller)# exit</pre>	Returns you to global configuration mode.
<b>Step 4</b>	<b>interface atm slot/subslot/port</b> <b>Example:</b> <pre>Router(config)# interface atm 0/3/0</pre>	Selects the ATM interface in Step 2.
<b>Step 5</b>	<b>pvc vpi/vci</b> <b>Example:</b> <pre>Router(config-if)# pvc 0/40</pre>	Configures a PVC for the interface and assigns the PVC a VPI and VCI. Do not specify 0 for both the VPI and VCI.
<b>Step 6</b>	<b>xconnect peer-router-id vcid {encapsulation mpls   pseudowire-class name}</b> <b>Example:</b> <pre>Router(config-if)# xconnect 10.10.2.204 200 encapsulation mpls</pre>	Configures a pseudowire to carry data from the clear-channel ATM interface over the MPLS network.
<b>Step 7</b>	<b>end</b> <b>Example:</b> <pre>Router(config-if)# end</pre>	Exits configuration mode.

# 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 53](#)
- [Configuring an IMA Interface, on page 54](#)
- [Configuring the ATM over MPLS Pseudowire Interface, on page 55](#)

## Configuring the Controller

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>card type {e1} slot/subslot</b> <b>Example:</b>  Router(config)# card type e1 0 0	Configures IMA on an E1 or T1 interface.
<b>Step 4</b>	<b>controller {e1} slot/subslot</b> <b>Example:</b>  Router(config)# controller e1 0/4	Specifies the controller interface on which you want to enable IMA.
<b>Step 5</b>	<b>clock source {internal   line}</b> <b>Example:</b>  Router(config-controller)# <b>clock source internal</b>	Sets the clock source to internal.
<b>Step 6</b>	<b>ima-group group-number scrambling-payload</b> <b>Example:</b>  Router(config-controller)# ima-group 0 scrambling-payload	If you want to configure an ATM IMA backhaul, use the <b>ima-group</b> command to assign the interface to an IMA group. For a T1 connection, use the <b>no-scrambling-payload</b> to disable ATM-IMA cell payload scrambling; for

	Command or Action	Purpose
		<p>an E1 connection, use the <b>scrambling-payload</b> parameter to enable ATM-IMA cell payload scrambling.</p> <p>The example assigns the interface to IMA group 0 and enables payload scrambling.</p>
<b>Step 7</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config)# exit</pre>	Exits configuration mode.

## 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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<p><b>interface ATM <i>slot</i> / IMA <i>group-number</i></b></p> <p><b>Example:</b></p> <pre>Router(config-controller)# interface atm0/ima0</pre> <p><b>Example:</b></p> <pre>Router(config-if)#</pre>	<p>Specifies the slot location and port of IMA interface group. The syntax is as follows:</p> <ul style="list-style-type: none"> <li>• <i>slot</i>—The slot location of the interface module.</li> <li>• <i>group-number</i>—The group number of the IMA group.</li> </ul> <p>The example specifies the slot number as 0 and the group number as 0.</p>

	Command or Action	Purpose
		<p><b>Note</b></p> <p>To explicitly configure the IMA group ID for the IMA interface, you may use the optional <b>ima group-id</b> 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.</p>
<b>Step 4</b>	<p><b>no ip address</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# no ip address</pre>	Disables the IP address configuration for the physical layer interface.
<b>Step 5</b>	<p><b>atm bandwidth dynamic</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# atm bandwidth dynamic</pre>	Specifies the ATM bandwidth as dynamic.
<b>Step 6</b>	<p><b>no atm ilmi-keepalive</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# no atm ilmi-keepalive</pre>	Disables the ILMI keepalive parameters.
<b>Step 7</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config)# exit</pre>	Exits configuration mode.

#### What to do next

For more information about configuring IMA groups, see the [Configuring ATM IMA, on page 46](#).

## Configuring the ATM over MPLS Pseudowire Interface

You can configure ATM over MPLS in 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 56](#)—Maps a single VCC to a single pseudowire
- [Configuring N-to-1 VCC Cell Transport Pseudowire, on page 57](#)—Maps multiple VCCs to a single pseudowire
- [Configuring 1-to-1 VPC Cell Transport, on page 57](#)—Maps a single VPC to a single pseudowire
- [Configuring ATM AAL5 SDU VCC Transport, on page 59](#)—Maps a single ATM PVC to another ATM PVC
- [Configuring a Port Mode Pseudowire, on page 60](#)—Maps one physical port to a single pseudowire connection
- [Optional Configurations, on page 61](#)



**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 10.10.10.2 255.255.255.255 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.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface ATM <i>slot</i> / IMA <i>group-number</i></b> <b>Example:</b> <pre>Router(config-controller)# interface atm0/ima0</pre>	Configures the ATM IMA interface.



	Command or Action	Purpose
<b>Step 4</b>	<b>pvc slot/subslot l2transport</b> <b>Example:</b>  Router(config-if-atm) # <b>pvc 0/40</b> <b>l2transport</b>	Defines a PVC. Use the <b>l2transport</b> keyword to configure the PVC as a layer 2 virtual circuit.
<b>Step 5</b>	<b>encapsulation aal0</b> <b>Example:</b>  Router(config-if-atm-l2trans-pvc) # encapsulation aal0	Defines the encapsulation type for the PVC. The default encapsulation type for the PVC is AAL5.
<b>Step 6</b>	<b>xconnect router_ip_address vcid encapsulation mpls</b> <b>Example:</b>  Router(config-if-atm-l2trans-pvc) # xconnect 10.0.0.1 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 10.0.0.1.
<b>Step 7</b>	<b>end</b> <b>Example:</b>  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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>	Enables privileged EXEC mode.  • Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface ATM slot / IMA group-number</b> <b>Example:</b> Router(config-controller)# interface atm0/ima0 <b>Example:</b> Router(config-if)# <b>Example:</b>	Configures the ATM IMA interface.
<b>Step 4</b>	<b>atm pvp vpi l2transport</b> <b>Example:</b> Router(config-if-atm)# <b>atm pvp 10 l2transport</b> <b>Example:</b> Router(config-if-atm-l2trans-pvp)#	Maps a PVP to a pseudowire.
<b>Step 5</b>	<b>xconnect peer-router-id vcid {encapsulation mpls}</b> <b>Example:</b> Router(config-if-atm-l2trans-pvp)# <b>xconnect 10.10.10.2 305 encapsulation mpls</b> <b>Example:</b> Router(config-if-atm-l2trans-pvp-xconn)#	Binds an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 305 to the remote peer 30.30.30.2.
<b>Step 6</b>	<b>end</b> <b>Example:</b> Router(config-if-atm-l2trans-pvp-xconn)# <b>end</b> <b>Example:</b>	Exits the configuration mode.

## 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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface ATM <i>slot / IMA group-number</i></b> <b>Example:</b> <pre>Router(config-controller)# interface atm0/ima0</pre> <b>Example:</b> <pre>Router(config-if)#</pre> <b>Example:</b>	Configures the ATM IMA interface.
<b>Step 4</b>	<b>atm pvp <i>vpi</i> l2transport</b> <b>Example:</b> <pre>Router(config-if)# pvc 0/12 l2transport</pre> <b>Example:</b> <pre>Router(config-if-atm-l2trans-pvc)#</pre>	Configures a PVC and specifies a VCI or VPI.
<b>Step 5</b>	<b>encapsulation aal5</b> <b>Example:</b> <pre>Router(config-if-atm-l2trans-pvc)# encapsulation aal5</pre>	Sets the PVC encapsulation type to AAL5. <b>Note</b> You must use the AAL5 encapsulation for this transport type.
<b>Step 6</b>	<b>xconnect <i>peer-router-id vcid</i> encapsulation mpls</b>	Binds an attachment circuit to the ATM IMA interface to create a pseudowire. This example

	Command or Action	Purpose
	<b>Example:</b> <pre>Router(config-if-atm-l2trans-pvc) # xconnect 10.10.10.2 125 encapsulation mpls</pre>	creates a pseudowire by binding the ATM circuit 125 to the remote peer 25.25.25.25.
<b>Step 7</b>	<b>exit</b> <b>Example:</b> <pre>Router(config)# exit</pre>	Exits configuration mode.

## Configuring a Port Mode Pseudowire

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

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface ATM <i>slot</i> / IMA <i>group-number</i></b> <b>Example:</b> <pre>Router(config-controller)# interface atm0/ima0</pre> <b>Example:</b> <pre>Router(config-if)#</pre> <b>Example:</b>	Configures the ATM interface.
<b>Step 4</b>	<b>xconnect <i>peer-router-id</i> <i>vcid</i> encapsulation mpls</b> <b>Example:</b> <pre>Router(config-if-atm-l2trans-pvc) #</pre>	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.

	Command or Action	Purpose
	<code>xconnect 10.10.10.2 125 encapsulation mpls</code>	
<b>Step 5</b>	<b>exit</b> <b>Example:</b>  <code>Router(config)# exit</code>	Exits configuration mode.

## 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.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  <code>Router# configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>interface ATM slot / IMA group-number</b> <b>Example:</b>  <code>Router(config-controller)# interface atm0/ima0</code> <b>Example:</b>  <code>Router(config-if)#</code>	Configures the ATM interface.
<b>Step 4</b>	<b>atm mcpt-timers timer1 timer2 timer3</b> <b>Example:</b>  <code>Router(config-if)# atm mcpt-timers 1000 2000 3000</code>	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.
<b>Step 5</b>	<b>atm pvp vpi l2transport</b> <b>Example:</b>	Configures a PVC and specifies a VCI or VPI.

	Command or Action	Purpose
	<pre>Router(config-if)# pvc 0/12 12transport</pre> <p><b>Example:</b></p> <pre>Router(config-if-atm-12trans-pvc)#</pre>	
<b>Step 6</b>	<p><b>encapsulation aal5</b></p> <p><b>Example:</b></p> <pre>Router(config-if-atm-12trans-pvc)# encapsulation aal5</pre>	<p>Sets the PVC encapsulation type to AAL5.</p> <p><b>Note</b> You must use the AAL5 encapsulation for this transport type.</p>
<b>Step 7</b>	<p><b>cell-packing</b> <i>maxcells</i> <b>mcpt-timer</b> <i>timer-number</i></p> <p><b>Example:</b></p> <pre>Router(config-if-atm-12trans-pvc)# cell-packing 20 mcpt-timer 3</pre>	<p>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.</p>
<b>Step 8</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Router(config-if-atm-12trans-pvc)# end</pre>	<p>Exits the configuration mode.</p>

## 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 39](#).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>

	Command or Action	Purpose
<b>Step 3</b>	<p><b>interface</b> <i>interface-id</i></p> <p><b>Example:</b></p> <pre>Router(config)# interface gigabitethernet 0/0/4</pre>	<p>Specifies the port on which to create the pseudowire and enters interface configuration mode. Valid interfaces are physical Ethernet ports.</p>
<b>Step 4</b>	<p><b>service instance</b> <i>number</i> <b>ethernet</b> [<i>name</i>]</p> <p><b>Example:</b></p> <pre>Router(config-if)# service instance 2 ethernet</pre>	<p>Configure an EFP (service instance) and enter service instance configuration) mode.</p> <ul style="list-style-type: none"> <li>• The <i>number</i> is the EFP identifier, an integer from 1 to 4000.</li> <li>• (Optional) <b>ethernet</b> <i>name</i> is the name of a previously configured EVC. You do not need to use an EVC name in a service instance.</li> </ul> <p><b>Note</b> 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/cether/configuration/xe-3s/asr903/ce-xe-3s-asr903-book/ce-vc.html">http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xe-3s/asr903/ce-xe-3s-asr903-book/ce-vc.html</a></p>
<b>Step 5</b>	<p><b>encapsulation</b> {<b>default</b>   <b>dot1q</b>   <b>priority-tagged</b>   <b>untagged</b>}</p> <p><b>Example:</b></p> <pre>Router(config-if-srv)# encapsulation dot1q 2</pre>	<p>Configure encapsulation type for the service instance.</p> <ul style="list-style-type: none"> <li>• <b>default</b>—Configure to match all unmatched packets.</li> <li>• <b>dot1q</b>—Configure 802.1Q encapsulation.</li> <li>• <b>priority-tagged</b>—Specify priority-tagged frames, VLAN-ID 0 and CoS value of 0 to 7.</li> <li>• <b>untagged</b>—Map to untagged VLANs. Only one EFP per port can have untagged encapsulation.</li> </ul>
<b>Step 6</b>	<p><b>xconnect</b> <i>peer-ip-address</i> <i>vc-id</i> {<b>encapsulation</b> {<b>l2tpv3</b> [<b>manual</b>]   <b>mpls</b> [<b>manual</b>]}   <b>pw-class</b> <i>pw-class-name</i> } [<b>pw-class</b> <i>pw-class-name</i>] [<b>sequencing</b> {<b>transmit</b>   <b>receive</b>   <b>both</b>}]</p> <p><b>Example:</b></p>	<p>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.</p>

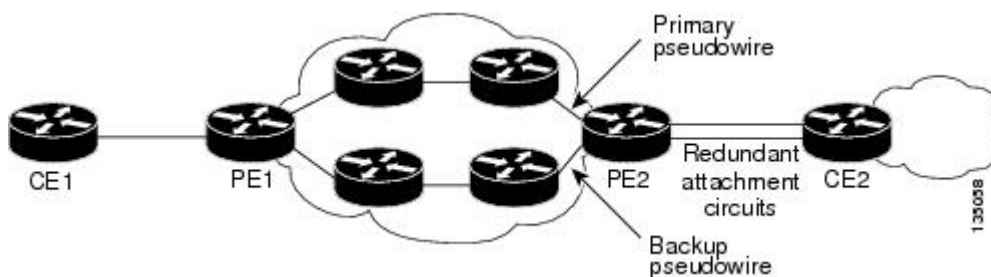
	Command or Action	Purpose
	<pre>Router (config-if-srv)# xconnect 10.1.1.2 101 encapsulation mpls</pre>	<b>Note</b> When creating IP routes for a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as <b>ip route 10.10.10.2 255.255.255.255 10.2.3.4</b> .
<b>Step 7</b>	<b>exit</b>  <b>Example:</b>  <pre>Router(config)# exit</pre>	Exits configuration mode.

## 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 64 shows an example of pseudowire redundancy.

Figure 3: Pseudowire Redundancy



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

Follow these steps to configure a backup peer:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>



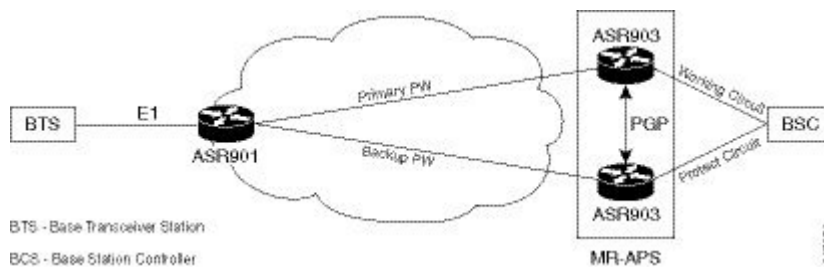
	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>pseudowire-class [pw-class-name]</b> <b>Example:</b>  Router(config)# pseudowire-class mpls	Specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.
<b>Step 4</b>	<b>encapsulation mpls</b> <b>Example:</b>  Router(config-pw-class)# encapsulation mpls	Specifies MPLS encapsulation.
<b>Step 5</b>	<b>interface serial slot/subslot/port</b> <b>Example:</b>  Router(config)# interface serial0/0	Enters configuration mode for the serial interface.  <b>Note</b> The slot number is always 0.
<b>Step 6</b>	<b>backup delay enable-delay {disable-delay   never}</b> <b>Example:</b>  Router(config)# backup delay 0 10	Configures the backup delay parameters. Where: <ul style="list-style-type: none"> <li>• <i>enable-delay</i>—Time before the backup PW takes over for the primary PW.</li> <li>• <i>disable-delay</i>—Time before the restored primary PW takes over for the backup PW.</li> <li>• <b>never</b>—Disables switching from the backup PW to the primary PW.</li> </ul>
<b>Step 7</b>	<b>xconnect router-id encapsulation mpls</b> <b>Example:</b>  Router(config-if)# <b>xconnect 10.10.10.2 101 encapsulation mpls</b>	Binds the Ethernet port interface to an attachment circuit to create a pseudowire.
<b>Step 8</b>	<b>backup peer peer-router-ip-address vcid [pw-class pw-class name]</b> <b>Example:</b>  Router(config)# backup peer 10.10.10.1 104 pw-class pw1	Defines the address and VC of the backup peer.
<b>Step 9</b>	<b>exit</b> <b>Example:</b>  Router(config)# <b>exit</b>	Exits configuration mode.

## 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 thereby coupled with the pseudowire status.

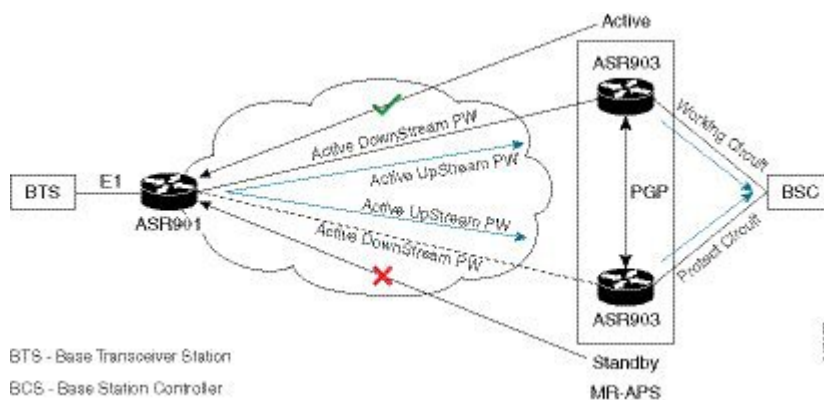
**Figure 4: Pseudowire Redundancy with MR-APS**



BSC monitors the status of the incoming signal from the working and protect routers. In the event of a switchover 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.

**Figure 5: Pseudowire Redundancy with Uni-directional Active-Active**






---

**Note** 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
|         Output modifiers
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 33](#)



**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
    xconnect 17.1.1.1 1101 encapsulation mpls pw-class pseudowire1
    !
  cem 1201
    xconnect 17.1.1.1 1201 encapsulation mpls pw-class pseudowire1
    !
  cem 1119
    xconnect 17.1.1.1 1119 encapsulation mpls pw-class pseudowire1
    !
  cem 1244
    xconnect 17.1.1.1 1244 encapsulation mpls pw-class pseudowire1
    !
  cem 1130
    xconnect 17.1.1.1 1130 encapsulation mpls pw-class pseudowire1
    !
  cem 1290
    xconnect 17.1.1.1 1290 encapsulation mpls pw-class pseudowire1

```

## BGP PIC Configuration

```

cef table output-chain build favor convergence-speed
!
router bgp 1
  bgp log-neighbor-changes
  bgp graceful-restart
  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 0
  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

```

## 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
  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
  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 33](#)




---

**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 10.0.0.1 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

```

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

```
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 ATM0/0/0.10 point
pvc 20/101 l2transport
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 192.168.37.3 100 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

```

## 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 l2transport
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 l2transport
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 0.0.255.255 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 ATM9/3/1.10 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 0.0.255.255 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 l2transport
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 0.0.255.255 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 l2transport
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 0.0.255.255 area 1
network 192.168.37.0 0.0.0.255 area 1
nsf

```

## 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  
!  
router 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  
!  
router 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  
!
```





## CHAPTER 4

# Configuring Multi Router Automatic Protection Switching

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.



**Note** When you perform protect-active router powercycle, the convergence times becomes high ranging from 2.3 seconds to 2.8 seconds. The APS switchover triggers the PWs at the protect interface to become active during any one of the following failure scenarios:

- Either port at the ADM does not respond.
- The port at the router does not respond.
- The link between ADM and router fails.
- The router fails over.

- [Restrictions for MR-APS, on page 81](#)
- [Information About MR-APS, on page 82](#)
- [Configuring MR-APS with HSPW-ICRM on a CEM interface, on page 84](#)
- [Configuring MR-APS on a POS interface, on page 97](#)

## 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.
- You can perform a force switchover to overcome the following limitations:
  - An interface module OIR, either through physical or software causes the APS switchover time to be higher (500-600ms).
  - Shut or no shut of the port may lead to higher APS switchover time.
  - Removal of the active working or protect interface may lead to higher APS switchover time.

## 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.

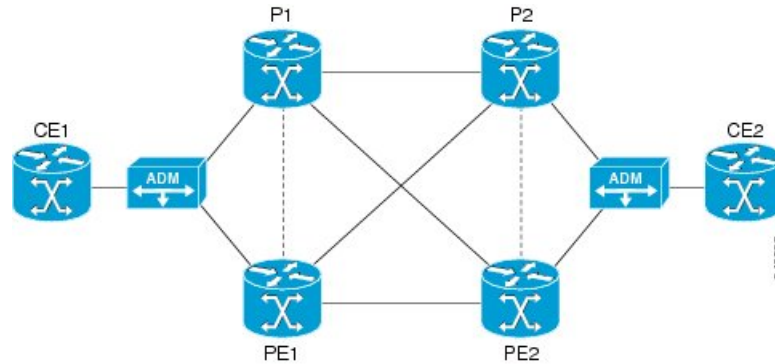
The HSPW support for TDM access circuits (ACs) allow the backup PW to be in a hot-standby state, so that it can immediately take over if the primary PW fails. The present HSPW solution does not support ACs as part of the APS group. The PWs which are configured over the protected interface, remain in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

Figure 6: MR-APS Integration with HSPW Implementation

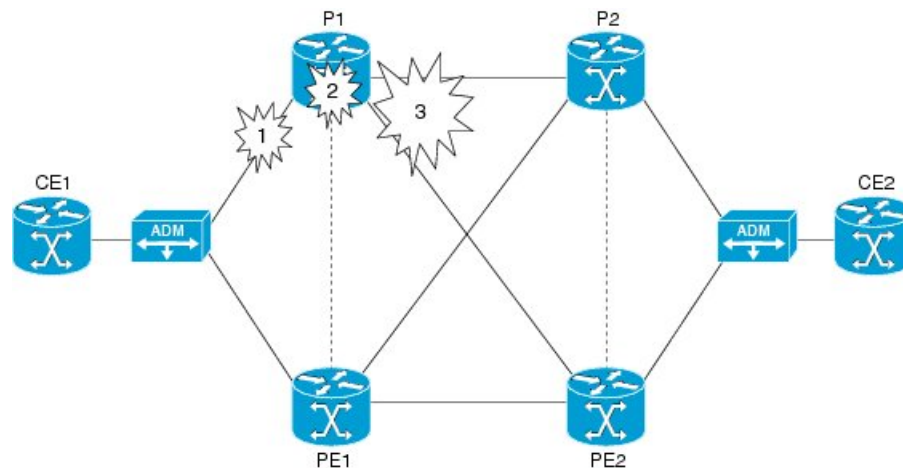


### Failover Operations

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.

Figure 7: Failure Points in the Network

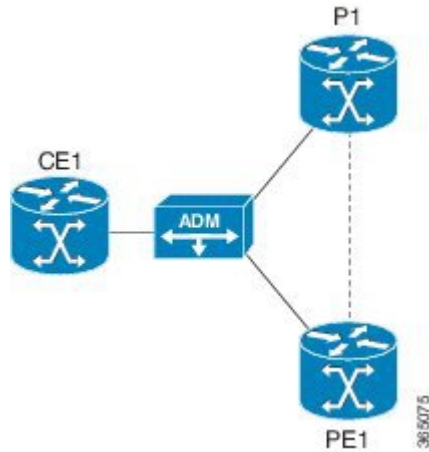


In case of failure 1, where either port at the ADM goes down, or the port at the router goes down, or the link between ADM and router fails, the APS switchover triggers the pseudowires at the protect interface to become active. The same applies to failure 2 as well where the complete router fails over.

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

APS switchover. The ICRM monitors the directly connected interfaces only. Hence only those failures in the directly connected interfaces can cause a core isolation event.

Figure 8: MR-APS Integration on a POS interface



## 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:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>pseudowire-class <i>pw-class-name</i></b> <b>Example:</b> Router (config)# <b>pseudowire-class</b> <b>hspw_aps</b>	Specifies the name of a PW class and enters PW class configuration mode.
<b>Step 4</b>	<b>encapsulation mpls</b> <b>Example:</b> Router (config-pw-class)# <b>encapsulation</b> <b>mpls</b>	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the PW.
<b>Step 5</b>	<b>status peer topology dual-homed</b> <b>Example:</b>	Enables the reflection of the attachment circuit status on both the primary and secondary PWs.

	Command or Action	Purpose
	<code>Router(config-pw-class)# status peer topology dual-homed</code>	This configuration is necessary if the peer PEs are connected to a dual-homed device.
<b>Step 6</b>	<b>exit</b> <b>Example:</b> <code>Router(config-pw-class)# exit</code>	Exits PW class configuration mode.
<b>Step 7</b>	<b>redundancy</b> <b>Example:</b> <code>Router(config)# redundancy</code>	Enters the redundancy configuration mode.
<b>Step 8</b>	<b>interchassis group <i>group-id</i></b> <b>Example:</b> <code>Router(config-red)# interchassis group 50</code>	Configures an interchassis group within the redundancy configuration mode and enters the interchassis redundancy mode.
<b>Step 9</b>	<b>member ip <i>ip-address</i></b> <b>Example:</b> <code>Router(config-r-ic)# member ip 60.60.60.2</code>	Configures the IP address of the peer member group.
<b>Step 10</b>	<b>backbone interface <i>slot/bay/port</i></b> <b>Example:</b> <code>Router(config-r-ic)#</code>	Specifies the backbone interface. <ul style="list-style-type: none"> <li>• <i>slot</i>—Chassis slot number, which is always 0.</li> <li>• <i>port</i>—Port or interface number. The range is from 0 to 7 for Gigabit Ethernet.</li> </ul>
<b>Step 11</b>	<b>exit</b> <b>Example:</b> <code>Router(config-r-ic)# exit</code>	Exits the redundancy mode.
<b>Step 12</b>	<b>controller SONET <i>slot/bay/port</i></b> <b>Example:</b> <code>Router(config)# controller SONET 0/5/2</code>	Selects and configures a SONET controller and enters controller configuration mode. <ul style="list-style-type: none"> <li>• <i>slot</i>—Chassis slot number, which is always 0.</li> <li>• <i>port</i>—Port or interface number. The range is from 0 to 7 for Gigabit Ethernet.</li> </ul>
<b>Step 13</b>	<b>framing [SDH   SONET]</b> <b>Example:</b> <code>Router(config-controller)# framing SONET</code>	Configures the controller with framing type. SONET framing is the default option.
<b>Step 14</b>	<b>clock source line</b> <b>Example:</b>	Sets the clocking for individual T1 or E1 links.

	Command or Action	Purpose
	Router (config-controller)# <b>clock source line</b>	
<b>Step 15</b>	<b>sts-1</b> <i>sts1-number</i>  <b>Example:</b> Router (config-controller)# <b>sts-1 1</b>	Specifies the STS identifier.
<b>Step 16</b>	<b>mode vt-15</b>  <b>Example:</b> Router (config-ctrlr-sts1)# <b>mode vt-15</b>	Specifies the STS-1 mode of operation.
<b>Step 17</b>	<b>vtg</b> <i>vtg_number</i> <b>t1</b> <i>t1_line_number</i> <b>cem-group</b> <i>group-number</i> <b>timeslots</b> <i>time-slot-range</i>  <b>Example:</b> Router (config-ctrlr-sts1)# <b>vtg 1 t1 1 cem-group 0 timeslots 1-24</b>	Creates a Circuit Emulation Services over Packet Switched Network circuit emulation (CESoPSN) CEM group. <ul style="list-style-type: none"> <li>• <b>vtg</b>—Specifies the VTG number from 1-7.</li> <li>• <b>t1</b>—Specifies the T1 line.</li> <li>• <b>t1_line_number</b>—Specifies the T1 line number.</li> <li>• <b>cem-group</b>—Creates a circuit emulation (CEM) channel from one or more time slots of a T1 line.</li> <li>• <b>group-number</b>—CEM identifier to be used for this group of time slots. For T1 ports, the range is from 0 to 23.</li> <li>• <b>timeslots</b>—Specifies that a list of time slots is to be used as specified by the <i>time-slot-range</i> argument.</li> <li>• <b>time-slot-range</b>—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.</li> </ul>
<b>Step 18</b>	<b>exit</b>  <b>Example:</b> Router (config-ctrlr-sts1)# <b>exit</b>	Exits from the STS configuration mode.
<b>Step 19</b>	<b>aps group</b> <i>group_id</i>  <b>Example:</b> Router (config-controller)# <b>aps group 1</b>	Configures the APS group for CEM.

	Command or Action	Purpose
<b>Step 20</b>	<b>aps</b> [ <b>working</b>   <b>protect</b> ] <i>aps-group-number</i> <b>Example:</b> <pre>Router(config-controller)# <b>aps working</b> 1</pre>	Configures the APS group as working or protect interface.  <b>Note</b> For MR-APS, one router must be configured as <code>aps working 1</code> and the other router must be configured as <code>aps protect 1</code> .
<b>Step 21</b>	<b>aps hspw-icrm-grp</b> <i>group-number</i> <b>Example:</b> <pre>Router(config-controller)# <b>aps</b> <b>hspw-icrm-group 1</b></pre>	Associates the APS group to an ICRM group number.
<b>Step 22</b>	<b>exit</b> <b>Example:</b> <pre>Router(config-controller)# <b>exit</b></pre>	Ends the controller session and returns to the configuration mode.
<b>Step 23</b>	<b>interface cem</b> <i>slot/bay/port</i> <b>Example:</b> <pre>Router(config)# <b>interface cem 0/5/2</b></pre>	Configures a serial interface and enters the interface configuration mode <ul style="list-style-type: none"> <li>• <i>slot</i>—Chassis slot number, which is always 0.</li> <li>• <i>port</i>—Port or interface number. The range is from 0 to 7 for Gigabit Ethernet.</li> </ul>
<b>Step 24</b>	<b>cem</b> <i>group-number</i> <b>Example:</b> <pre>Router(config-if)# <b>cem 0</b></pre>	Selects the CEM circuit (group) to configure a PW for.
<b>Step 25</b>	<b>xconnect</b> <i>peer-ip-address vcid pw-class pw-class-name</i> <b>Example:</b> <pre>Router(config-if-srv)# <b>xconnect 3.3.3.3</b> <b>1 pw-class hspw_aps</b></pre>	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. <ul style="list-style-type: none"> <li>• <i>peer-ip-address</i>—IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.</li> <li>• <i>vcid</i>—32-bit identifier of the virtual circuit (VC) between the PE routers.</li> <li>• <b>pw-class</b>—Specifies the PW class.</li> <li>• <i>pw-class-name</i>—Specifies the name of the PW class.</li> </ul>

	Command or Action	Purpose
		<b>Note</b> The peer router IP address and virtual circuit ID must be a unique combination on the router.
<b>Step 26</b>	<b>backup peer</b> <i>peer-id</i> <i>vc-id</i> <b>pw-class</b> <i>pw-class-name</i>  <b>Example:</b> Router(config-if-srv)# <b>backup peer</b> 4.3.3.3 90 <b>pw-class</b> vpws	Specifies a redundant peer for a PW virtual circuit. <ul style="list-style-type: none"> <li>• <i>peer-id</i> <i>vc-id</i>—Specifies IP address of the remote peer.</li> <li>• <b>pw-class</b>—Specifies the PW class.</li> <li>• <i>pw-class-name</i>—Specifies the name of the PW class.</li> </ul>
<b>Step 27</b>	<b>end</b>  <b>Example:</b> Router(config-if-srv)# <b>end</b>	Returns to privileged EXEC mode.

## 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
```

```

CEM Int.      ID   Ctrlr   Admin   Circuit   AC
-----
          1   UP     UP     Active   UP
          2   UP     UP     Active   UP
          3   UP     UP     Active   UP
!
.
.
.
          83  UP     UP     Active   UP
          84  UP     UP     Active   UP
!

```

Following is a sample output of the **show cem circuit0-504** command to display the detailed information about that particular circuit:

```
Router# show cem circuit 1
```



```

, 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                    Severly Errored Sec:   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:
, 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:
, 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:

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

Local intf	Local circuit	Dest address	VC ID	Status
	SATOP T1 1	17.3.3.3	1001	UP
	SATOP T1 2	17.3.3.3	1002	UP
	SATOP T1 3	17.3.3.3	1003	UP
!				
.				
.				
	SATOP T1 19	17.3.3.3	1019	UP
	SATOP T1 20	17.3.3.3	1020	UP
!				

Local intf	Local circuit	Dest address	VC ID	Status
	SATOP T1 21	17.3.3.3	1021	UP
	SATOP T1 22	17.3.3.3	1022	UP
	SATOP T1 23	17.3.3.3	1023	UP
!				
.				
.				
	SATOP T1 25	17.3.3.3	1025	UP
	SATOP T1 43	17.3.3.3	1043	UP
!				

Local intf	Local circuit	Dest address	VC ID	Status
	SATOP T1 44	17.3.3.3	1044	UP
	SATOP T1 45	17.3.3.3	1045	UP
	SATOP T1 46	17.3.3.3	1046	UP
!				
.				
.				
	SATOP T1 65	17.3.3.3	1065	UP
	SATOP T1 66	17.3.3.3	1066	UP
!				

Local intf	Local circuit	Dest address	VC ID	Status
	SATOP T1 67	17.3.3.3	1067	UP

```

        SATOP T1 68                17.3.3.3        1068        UP
        SATOP T1 69                17.3.3.3        1069        UP
!
.
.
.
        SATOP T1 83                17.3.3.3        1083        UP
        SATOP T1 84                17.3.3.3        1084        UP
STANDBY SATOP T1 1                17.4.4.4        4001
STANDBY SATOP T1 2                17.4.4.4        4002
STANDBY SATOP T1 3                17.4.4.4        4003
STANDBY SATOP T1 4                17.4.4.4        4004
STANDBY SATOP T1 5                17.4.4.4        4005
!
Local intf      Local circuit      Dest address      VC ID      Status
-----
STANDBY SATOP T1 6        17.4.4.4        4006
STANDBY SATOP T1 7        17.4.4.4        4007
STANDBY SATOP T1 8        17.4.4.4        4008
!
.
.
.
STANDBY SATOP T1 27        17.4.4.4        4027
STANDBY SATOP T1 28        17.4.4.4        4028
!
Local intf      Local circuit      Dest address      VC ID      Status
-----
STANDBY SATOP T1 29        17.4.4.4        4029
STANDBY SATOP T1 30        17.4.4.4        4030
STANDBY SATOP T1 31        17.4.4.4        4031
!
.
.
.

```

```

STANDBY          SATOP T1 50          17.4.4.4          4050
STANDBY          SATOP T1 51          17.4.4.4          4051
STANDBY
!
Local intf      Local circuit      Dest address      VC ID      Status
-----
STANDBY          SATOP T1 52          17.4.4.4          4052
STANDBY          SATOP T1 53          17.4.4.4          4053
STANDBY          SATOP T1 54          17.4.4.4          4054
STANDBY
!
.
.
.
STANDBY          SATOP T1 73          17.4.4.4          4073
STANDBY          SATOP T1 74          17.4.4.4          4074
STANDBY
!
Local intf      Local circuit      Dest address      VC ID      Status
-----
STANDBY          SATOP T1 75          17.4.4.4          4075
STANDBY          SATOP T1 76          17.4.4.4          4076
STANDBY          SATOP T1 77          17.4.4.4          4077
STANDBY
!
.
.
.
STANDBY          SATOP T1 83          17.4.4.4          4083
STANDBY          SATOP T1 84          17.4.4.4          4084
STANDBY
!
R-96-2011#sh cem circuit
CEM Int.      ID   Ctrlr   Admin   Circuit   AC
-----
          1   UP     UP     Active   UP
          2   UP     UP     Active   UP
          3   UP     UP     Active   UP
!
.
.
.
          83  UP     UP     Active   UP

```

```

      84   UP       UP       Active       UP
!

```

- 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:      up, line protocol up, SATOP T1 1 up
Destination address: 17.3.3.3, VC ID: 1001, VC status: up
Output interface:    , 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
```



```

.
.
UP pri    ac   :9(SATOP T1)          UP mpls 17.3.3.3:1009
  UP
IA sec    ac   :9(SATOP T1)          UP mpls 17.4.4.4:4009
  SB
!

```

## 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
RouterP1(config-r-ic)# backbone interface
RouterP1(config-r-ic)# exit
RouterP1(config)# controller SONET
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 t1 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
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
RouterP1(config-if)# exit
RouterP1(config)# end

```

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-r-ic)# member ip 14.2.0.1
RouterPE1(config-r-ic)# backbone interface
RouterPE1(config-r-ic)# backbone interface
RouterPE1(config-r-ic)# exit
RouterPE1(config)# controller SONET

```

```

RouterPE1(config-controller)# framing sonet
RouterPE1(config-controller)# clock source line
RouterPE1(config-controller)# sts-1 1
RouterPE1(config-ctrlr-sts1)# mode vt-15
RouterPE1(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterPE1(config-ctrlr-sts1)# 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
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-r-ic)# member ip 14.6.0.2
RouterP2(config-r-ic)# backbone interface
RouterP2(config-r-ic)# backbone interface
RouterP2(config-r-ic)# exit
RouterP2(config)# controller SONET
RouterP2(config-controller)# framing sonet
RouterP2(config-controller)# clock source line
RouterP2(config-controller)# sts-1 1
RouterP2(config-ctrlr-sts1)# mode vt-15
RouterP2(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterP2(config-ctrlr-sts1)# exit
RouterP2(config-controller)# aps group 3
RouterP2(config-controller)# aps working 1
RouterP2(config-controller)# aps hspw-icrm-grp 1
RouterP2(config-controller)# exit
RouterP2(config)# interface cem
RouterP2(config-if)# cem 0
RouterP2(config-if)# xconnect 10.1.1.1 1 encapsulation mpls pw-class hspw_aps
RouterP2(config-if)# backup peer 2.2.2.2 3 pw-class hspw_aps
RouterP2(config-if)# exit
RouterP2(config)# end

```

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 PE2:

```

RouterPE2> enable
RouterPE2# configure terminal
RouterPE2(config)# pseudowire-class hspw_aps
RouterPE2(config-pw-class)# encapsulation mpls
RouterPE2(config-pw-class)# status peer topology dual-homed
RouterPE2(config-pw-class)# exit
RouterPE2(config)# redundancy
RouterPE2(config-red)# interchassis group 1
RouterPE2(config-r-ic)# member ip 14.6.0.1
RouterPE2(config-r-ic)# backbone interface
RouterPE2(config-r-ic)# backbone interface
RouterPE2(config-r-ic)# exit

```



```

RouterPE2(config)# controller SONET
RouterPE2(config-controller)# framing sonet
RouterPE2(config-controller)# clock source line
RouterPE2(config-controller)# sts-1 1
RouterPE2(config-ctrlr-sts1)# mode vt-15
RouterPE2(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterPE2(config-ctrlr-sts1)# exit
RouterPE2(config-controller)# aps group 2
RouterPE2(config-controller)# aps protect 1 14.6.0.2
RouterPE2(config-controller)# aps hspw-icrm-grp 1
RouterPE2(config-controller)# exit
RouterPE2(config)# interface cem
RouterPE2(config-if)# cem 0
RouterPE2(config-if)# xconnect 10.1.1.1 2 pw-class hspw_aps
RouterPE2(config-if)# backup peer 2.2.2.2 4 pw-class hspw_aps
RouterPE2(config-if)# exit
RouterPE2(config)# end

```

## 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:

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>exit</b> <b>Example:</b> Router(config-pw-class)# <b>exit</b>	Exits PW class configuration mode.
<b>Step 4</b>	<b>redundancy</b> <b>Example:</b> Router(config)# <b>redundancy</b>	Enters the redundancy configuration mode.
<b>Step 5</b>	<b>interchassis group</b> <i>group-id</i> <b>Example:</b> Router(config-red)# <b>interchassis group</b> 50	Configures an interchassis group within the redundancy configuration mode and enters the interchassis redundancy mode.

	Command or Action	Purpose
<b>Step 6</b>	<b>member ip</b> <i>ip-address</i> <b>Example:</b> Router(config-r-ic)# <b>member ip</b> 60.60.60.2	Configures the IP address of the peer member group.
<b>Step 7</b>	<b>monitor peer</b> <i>bfd</i> <b>Example:</b> Router(config-red)# <b>monitor peer bfd</b>	Enables BFD on the POS link.
<b>Step 8</b>	<b>exit</b> <b>Example:</b> Router(config-r-ic)# <b>exit</b>	Exits the redundancy mode.
<b>Step 9</b>	<b>controller SONET</b> <i>slot/bay/port</i> <b>Example:</b> Router(config)# <b>controller SONET</b> 0/5/2	Selects and configures a SONET controller and enters controller configuration mode. <ul style="list-style-type: none"> <li>• <i>slot</i>—Chassis slot number, which is always 0.</li> <li>• <i>port</i>—Port or interface number. The range is from 0 to 7 for Gigabit Ethernet.</li> </ul>
<b>Step 10</b>	<b>framing</b> [SDH   SONET] <b>Example:</b> Router(config-controller)# <b>framing SONET</b>	Configures the controller with framing type. SONET framing is the default option.
<b>Step 11</b>	<b>clock source internal</b> <b>Example:</b> Router(config-controller)# <b>clock source internal</b>	Sets the clocking for individual E1 links.
<b>Step 12</b>	<b>sts-1</b> <i>1-3POS</i> <b>Example:</b> Router(config-controller)# <b>sts-1 1-3</b>	Specifies the STS identifier.
<b>Step 13</b>	<b>exit</b> <b>Example:</b> Router(config-ctrlr-sts1)# <b>exit</b>	Exits from the STS configuration mode.
<b>Step 14</b>	<b>controller SONET</b> <i>slot/bay/port</i> <b>Example:</b> Router(config)# <b>controller SONET</b> 0/5/2	Selects and configures a SONET controller and enters controller configuration mode.
<b>Step 15</b>	<b>Shutdown</b> <b>Example:</b> Router(config)# <b>Shutdown</b>	Shut down the controller before APS configuration.

	Command or Action	Purpose
<b>Step 16</b>	<b>aps group</b> <i>group_id</i> <b>Example:</b> Router(config-controller)# <b>aps group</b> 1	Configures the APS group for POS.
<b>Step 17</b>	<b>aps working</b> <i>aps-group-number</i> <b>Example:</b> Router(config-controller)# <b>aps working</b> 1	Configures the APS group as working or protect interface. <b>Note</b> For MR-APS, one router must be configured as aps working 1 and the other router must be configured as aps protect 1.
<b>Step 18</b>	<b>aps interchassis group</b> <i>group-id</i> <b>Example:</b> Router(config-red)# <b>aps interchassis group</b> 50	Configures an aps inter chassis group.
<b>Step 19</b>	<b>no shut</b> <b>Example:</b> Router(config-controller)# <b>no shut</b>	Shut down the controller.
<b>Step 20</b>	<b>exit</b> <b>Example:</b> Router(config-controller)# <b>exit</b>	Ends the controller session and returns to the configuration mode.
<b>Step 21</b>	<b>interface POS</b> <i>slot/bay/port</i> <b>Example:</b> Router(config)# <b>interface POS</b> 0/5/2	Configures a serial interface and enters the interface configuration mode <ul style="list-style-type: none"> <li>• <i>slot</i>—Chassis slot number, which is always 0.</li> <li>• <i>port</i>—Port or interface number. The range can be 0-3.</li> </ul>
<b>Step 22</b>	<b>ip address</b> <i>ip-address</i> <b>Example:</b> Router(config-if)# <b>ip address</b> 45.1.1.2 255.255.255.0	Assigns the ip address to POS interface
<b>Step 23</b>	<b>encapsulation</b> <i>ppp</i> <b>Example:</b> Router(config-if-srv)# <b>encapsulation</b> PPP	Specifies the ppp encapsulation over POS interface.
<b>Step 24</b>	<b>end</b> <b>Example:</b> Router(config-if-srv)# <b>end</b>	Returns to privileged EXEC mode.

## Configuring protect node for POS MR-APS

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

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>exit</b> <b>Example:</b> Router (config-pw-class) # <b>exit</b>	Exits PW class configuration mode.
<b>Step 4</b>	<b>redundancy</b> <b>Example:</b> Router (config) # <b>redundancy</b>	Enters the redundancy configuration mode.
<b>Step 5</b>	<b>interchassis group <i>group-id</i></b> <b>Example:</b> Router (config-red) # <b>interchassis group</b> 50	Configures an interchassis group within the redundancy configuration mode and enters the interchassis redundancy mode.
<b>Step 6</b>	<b>member ip <i>ip-address</i></b> <b>Example:</b> Router (config-r-ic) # <b>member ip</b> 60.60.60.2	Configures the IP address of the peer member group.
<b>Step 7</b>	<b>monitor peer <i>bfd</i></b> <b>Example:</b> Router (config-red) # <b>monitor peer bfd</b>	Enables BFD on the POS link.
<b>Step 8</b>	<b>exit</b> <b>Example:</b> Router (config-r-ic) # <b>exit</b>	Exits the redundancy mode.
<b>Step 9</b>	<b>controller SONET <i>slot/bay/port</i></b> <b>Example:</b> Router (config) # <b>controller SONET</b> 0/5/2	Selects and configures a SONET controller and enters controller configuration mode. <ul style="list-style-type: none"><li>• <i>slot</i>—Chassis slot number, which is always 0.</li></ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li><i>port</i>—Port or interface number. The range is from 0 to 7 for Gigabit Ethernet.</li> </ul>
<b>Step 10</b>	<b>framing</b> [SDH   SONET] <b>Example:</b> Router(config-controller)# <b>framing</b> SONET	Configures the controller with framing type. SONET framing is the default option.
<b>Step 11</b>	<b>clock source internal</b> <b>Example:</b> Router(config-controller)# <b>clock source internal</b>	Sets the clocking for individual E1 links.
<b>Step 12</b>	<b>sts-1 1-3POS</b> <b>Example:</b> Router(config-controller)# <b>sts-1 1-3</b>	Specifies the STS identifier.
<b>Step 13</b>	<b>exit</b> <b>Example:</b> Router(config-ctrlr-sts1)# <b>exit</b>	Exits from the STS configuration mode.
<b>Step 14</b>	<b>controller SONET slot/bay/port</b> <b>Example:</b> Router(config)# <b>controller SONET 0/5/2</b>	Selects and configures a SONET controller and enters controller configuration mode.
<b>Step 15</b>	<b>Shutdown</b> <b>Example:</b> Router(config)# <b>Shutdown</b>	Shut down the controller before APS configuration.
<b>Step 16</b>	<b>aps group group_id</b> <b>Example:</b> Router(config-controller)# <b>aps group 1</b>	Configures the APS group for POS.
<b>Step 17</b>	<b>aps protect 1 remote loopback ip</b> <b>Example:</b> Router(config-controller)# <b>aps protect 1 192.168.1.1</b>	Enable the protect node.
<b>Step 18</b>	<b>aps interchasis group interchasis group-id</b> <b>Example:</b> Router(config-controller)# <b>aps interchasis group 1</b>	Enable the inter chasis.
<b>Step 19</b>	<b>no shut</b> <b>Example:</b> Router(config-controller)# <b>no shut</b>	Unshut the controller.

	Command or Action	Purpose
<b>Step 20</b>	<b>exit</b> <b>Example:</b> Router(config-controller)# <b>exit</b>	Ends the controller session and returns to the configuration mode.
<b>Step 21</b>	<b>interface POS slot/bay/port</b> <b>Example:</b> Router(config)# <b>interface POS 0/5/2</b>	Configures a serial interface and enters the interface configuration mode <ul style="list-style-type: none"> <li>• <i>slot</i>—Chassis slot number, which is always 0.</li> <li>• <i>port</i>—Port or interface number. The range can be 0-3.</li> </ul>
<b>Step 22</b>	<b>ip address ip-address</b> <b>Example:</b> Router(config-if)# <b>ip address 45.1.1.2 255.255.255.0</b>	Assigns the ip address to POS interface
<b>Step 23</b>	<b>encapsulation ppp</b> <b>Example:</b> Router(config-if-srv)# <b>encapsulation PPP</b>	Specifies the ppp encapsulation over POS interface.
<b>Step 24</b>	<b>end</b> <b>Example:</b> Router(config-if-srv)# <b>end</b>	Returns to privileged EXEC mode.

## 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
aps_bulk: 0
aps_stby: 0
peer_stby: 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      : 0x80000006
AAA ID          : 14
Access IE       : 0xA0000006
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

ASR903_PE2#
```

- 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-interface)#ip address 45.1.1.2
RouterPE1(config-interface)#encapsulation ppp
RouterPE1(config)# redundancy
RouterPE1(config-red)# interchassis group 1
RouterPE1(config-r-ic)# member ip 14.2.0.2
RouterPE1(config-r-ic)# backbone interface gig 0/0/1
RouterPE1(config-r-ic)# exit

```

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 10.1.1.1
RouterPE2(config-controller)#aps interchassis group 1
RouterPE2(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
RouterPE3(config-interface)#encapsulation ppp
RouterPE3(config-controller)#network-clock input-source 1 controller SONET 0/4/2
RouterPE1(config-controller)#exit
```





## CHAPTER 5

# Hot Standby Pseudowire Support for ATM and TDM Access Circuits

---

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.

- [Prerequisites for Hot Standby Pseudowire Support for ATM and TDM Access Circuits, on page 107](#)
- [Restrictions for Hot Standby Pseudowire Support for ATM and TDM Access Circuits, on page 108](#)
- [Information About Hot Standby Pseudowire Support for ATM and TDM Access Circuits, on page 108](#)
- [How to Configure Hot Standby Pseudowire Support for ATM and TDM Access Circuits, on page 109](#)
- [Configuration Examples for Hot Standby Pseudowire Support for ATM and TDM Access Circuits, on page 114](#)
- [Additional References, on page 118](#)

## 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.
- 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.

## 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



---

**Note** Pseudowire for Static VPLS is *not* supported.

---

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).



**Note** 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

12 vfi config manual
   vpn id 1000
   ! Incomplete point-to-multipoint vfi config
```

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>template type pseudowire name</b> <b>Example:</b>  Device(config)# template type pseudowire static-vpls	Specifies the template type as pseudowire and enters template configuration mode.
<b>Step 4</b>	<b>encapsulation mpls</b> <b>Example:</b>  Device(config-template)# encapsulation mpls	Specifies the tunneling encapsulation.  • For Any Transport over MPLS (AToM), the encapsulation type is MPLS.
<b>Step 5</b>	<b>signaling protocol none</b> <b>Example:</b>  Device(config-template)# signaling protocol none	Specifies that no signaling protocol is configured for the pseudowire class.
<b>Step 6</b>	<b>preferred-path interface Tunnel-tp interface-number</b> <b>Example:</b>  Device(config-template)# preferred-path interface Tunnel-tp 1	(Optional) Specifies the path that traffic uses: an MPLS Traffic Engineering (TE) tunnel or destination IP address and Domain Name Server (DNS) name.

	Command or Action	Purpose
<b>Step 7</b>	<b>exit</b> <b>Example:</b>  Device(config-template)# exit	Exits template configuration mode and returns to global configuration mode.
<b>Step 8</b>	<b>interface pseudowire <i>number</i></b> <b>Example:</b>  Device(config)# interface pseudowire 1	Establishes a pseudowire interface and enters interface configuration mode.
<b>Step 9</b>	<b>source template type pseudowire <i>name</i></b> <b>Example:</b>  Device(config-if)# source template type pseudowire static-vpls	Configures the source template type of the configured pseudowire.
<b>Step 10</b>	<b>neighbor <i>peer-address vcid-value</i></b> <b>Example:</b>  Device(config-if)# neighbor 10.0.0.1 123	Specifies the peer IP address and VC ID value of a Layer 2 VPN (L2VPN) pseudowire.
<b>Step 11</b>	<b>label <i>local-pseudowire-label remote-pseudowire-label</i></b> <b>Example:</b>  Device(config-if)# label 301 17	Configures an Any Transport over MPLS (AToM) static pseudowire connection by defining local and remote circuit labels.
<b>Step 12</b>	<b>end</b> <b>Example:</b>  Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

## 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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface atm number</b> <b>Example:</b>  Router(config)# interface atm4/1/0	Specifies the ATM interface and enters interface configuration mode.
<b>Step 4</b>	<b>pvc [name] vpi/vci l2transport</b> <b>Example:</b>  Router(config-if)# pvc 1/100 l2transport	Creates or assigns a name to an ATM PVC and enters L2transport PVC configuration mode.
<b>Step 5</b>	<b>xconnect peer-router-id vcid {encapsulation mpls  pw-class pw-class-name}</b> <b>Example:</b>  Router(config-if-atm-l2trans-pvc)# xconnect 10.0.0.1 123 pw-class atom	Binds the attachment circuit to a pseudowire VC.
<b>Step 6</b>	<b>backup peer peer-router-ip-addr vcid [pw-class pw-class-name]</b> <b>Example:</b>  Router(config-if-atm-l2trans-pvc)# backup peer 10.0.0.3 125 pw-class atom	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 <b>backup peer</b> command than the name that you used in the primary <b>xconnect</b> command.
<b>Step 7</b>	<b>backup delay enable-delay {disable-delay   never}</b> <b>Example:</b>  Router(config-if-atm-l2trans-pvc)# backup delay 5 never	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 <b>never keyword</b> , the primary pseudowire VC never takes over for the backup.

## 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.



## Procedure

### 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   Cktttype  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

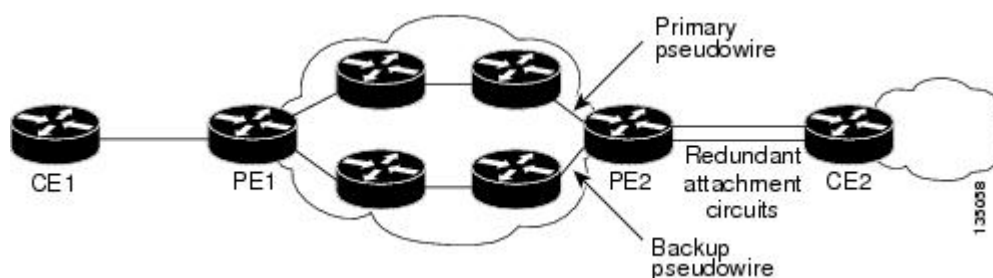
CEM3/0/0  Cemid 1
PW Ckt_type: 19 Aie hdl: EE00000B Peer aie hdl: 0x2000000C
Switch hdl: 0xB00E Segment hdl: 0x201E Redundancy Switch hdl: 0x1000 Redundancy
Segment hdl: 0x4002 Redundancy Member Prov: Yes
```

# 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*

25P



**2EP**

```

scrh
msc
scrh
0
tni
scrh
scrh
scrh
scrh
scrh
nca
scrh
tni
nca
scrh
scrh
221
scrh
505
441
scrh
005
nca
scrh
scrh
!
nca
scrh
scrh
5
scrh
441
505
scrh
scrh
scrh

```

Table 5: Configuring Hot Standby Pseudowire Support for ATM and TDM Access Circuits on ATM Circuits: Example

PE1	PE2
<pre>interface Loopback0  ip address 10.44.44.44 255.255.255.255 ! interface POS3/3/0  ip address 10.4.4.4 255.255.255.0  mpls ip ! interface ATM4/1/0  no ip address  no atm enable-ilmi-trap  pvc 1/100 l2transport   xconnect 10.22.22.22 1 encapsulation mpls   backup peer 10.22.22.22 2</pre>	<pre>interface Loopback0  ip address 10.22.22.22 255.255.255.255 ! interface POS3/3/0  ip address 10.4.4.1 255.255.255.0  mpls ip ! interface ATM4/1/0  no ip address  no atm enable-ilmi-trap  pvc 1/100 l2transport   xconnect 10.44.44.44 1 encapsulation mpls !  pvc 1/200 l2transport   xconnect 10.44.44.44 2 encapsulation mpls</pre>

## Additional References

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

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
MPLS commands	<i>Cisco IOS Multiprotocol Label Switching Command Reference</i>

### Standards

Standard	Title
draft-muley-pwe3-redundancy	Pseudowire Redundancy
draft-ietf-pwe3-iccp-xx.txt	Inter-Chassis Communication Protocol for L2VPN PE Redundancy

### MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>CISCO-IETF-PW-ATM-MIB</li> </ul>	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>

**RFCs**

<b>RFC</b>	<b>Title</b>
RFC 5085	Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires

**Technical Assistance**

<b>Description</b>	<b>Link</b>
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>

Additional References





## CHAPTER 6

# PPP and Multilink PPP Configuration

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 121](#)
- [PPP and Multilink PPP, on page 122](#)
- [IP Address Pooling, on page 123](#)
- [How to Configure PPP, on page 125](#)
- [Monitoring and Maintaining PPP and MLP Interfaces, on page 144](#)

## 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:

- Dialer map lookup—This method is used only if the peer requests an IP address, no other peer IP address has been assigned, and the interface is a member of a dialer group.

- PPP EXEC command—An asynchronous dialup user can enter a peer IP address or hostname when PPP is invoked from the command line. The address is used for the current session and then discarded.
- IPCP negotiation—If the peer presents a peer IP address during IPCP address negotiation and no other peer address is assigned, the presented address is acknowledged and used in the current session.
- Default IP address.
- TACACS+ assigned IP address—During the authorization phase of IPCP address negotiation, TACACS+ can return an IP address that the user being authenticated on a dialup interface can use. This address overrides any default IP address and prevents pooling from taking place.
- DHCP retrieved IP address—If configured, the routers acts as a proxy client for the dialup user and retrieves an IP address from a DHCP server. That address is returned to the DHCP server when the timer expires or when the interface goes down.
- Local address pool—The local address pool contains a set of contiguous IP addresses (a maximum of 1024 addresses) stored in two queues. The free queue contains addresses available to be assigned and the used queue contains addresses that are in use. Addresses are stored to the free queue in first-in, first-out (FIFO) order to minimize the chance the address will be reused, and to allow a peer to reconnect using the same address that it used in the last connection. If the address is available, it is assigned; if not, another address from the free queue is assigned.
- Chat script (asynchronous serial interfaces only)—The IP address in the **dialer map** command entry that started the script is assigned to the interface and overrides any previously assigned peer IP address.
- Virtual terminal/protocol translation—The translate command can define the peer IP address for a virtual terminal (pseudo asynchronous interface).
- The pool configured for the interface is used, unless TACACS+ returns a pool name as part of authentication, authorization, and accounting (AAA). If no pool is associated with a given interface, the global pool named default is used.

## 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.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  <code>Router&gt; enable</code>	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  <code>Router# configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>interface serial <i>slot/subslot/port:channel</i></b> <b>Example:</b>  <code>Router(config)# interface serial 0/0/0:0</code>	Enters interface configuration mode.
<b>Step 4</b>	<b>encapsulation ppp</b> <b>Example:</b>  <code>Router(config-if) # encapsulation ppp</code>	Enables PPP encapsulation.  <b>Note</b> PPP echo requests are used as keepalives to minimize disruptions to the end users of your network. Use the <b>no keepalive</b> command to disable echo requests.
<b>Step 5</b>	<b>end</b> <b>Example:</b>  <code>Router(config-if)# end</code>	Exits interface configuration mode.

# Enabling CHAP or PAP Authentication

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<b>Step 3</b>	<p><b>interface serial <i>number</i></b></p> <p><b>Example:</b></p> <pre>Router(config)# interface serial 0/0/0</pre>	<p>Enters Interface Configuration mode.</p>
<b>Step 4</b>	<p><b>ppp authentication {chap   chap pap   pap chap   pap} [if-needed] [list-name   default] [callin]</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# ppp authentication chap</pre>	<p>Defines the authentication methods supported and the order in which they are used.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Use the <b>ppp authentication chap</b> command only with TACACS or extended TACACS.</li> <li>• With AAA configured on the router and list names defined for AAA, the <i>list-name</i> optional argument can be used with AAA/TACACS+. Use the <b>ppp use-tacacs</b> command with TACACS and Extended TACACS. Use the <b>aaa authentication ppp</b> command with AAA/TACACS+.</li> </ul>
<b>Step 5</b>	<p><b>ppp use-tacacs [single-line] or aaa authentication ppp</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# ppp use-tacacs single-line Router(config-if)# aaa authentication ppp</pre>	<p>Configure TACACS on a specific interface as an alternative to global host authentication.</p>

	Command or Action	Purpose
<b>Step 6</b>	<b>exit</b> <b>Example:</b> <pre>Router(config-if)# exit</pre>	Exits interface configuration mode.
<b>Step 7</b>	<b>username name [user-maxlinks link-number]</b> <b>password secret</b> <b>Example:</b> <pre>Router(config)# username name user-maxlinks 1 password password1</pre>	Configures identification. <ul style="list-style-type: none"> <li>• Optionally, you can specify the maximum number of connections a user can establish.</li> <li>• To use the <b>user-maxlinks</b> keyword, you must also use the <b>aaa authorization network default local</b> command and PPP encapsulation and name authentication on all the interfaces the user will be accessing.</li> </ul>
<b>Step 8</b>	<b>end</b> <b>Example:</b> <pre>Router(config)# end</pre>	Exits global configuration mode and enters privileged EXEC mode.  <b>Caution</b> If you use a list name that has not been configured with the <b>aaa authentication ppp</b> command, you disable PPP on the line.

### Example

```
Router# configure terminal
Router(config)# interface serial 0/0/0
Router(config-if)# ppp authentication chap
Router(config-if)# aaa authentication ppp
Router(config-if)# exit
Router(config)# username name user-maxlinks 1 password password1
Router(config)# end
```

## 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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip address-pool dhcp-proxy-client</b> <b>Example:</b> Router(config)# ip address-pool dhcp-proxy-client	Specifies the DHCP client-proxy feature as the global default mechanism. <ul style="list-style-type: none"> <li>• The <b>peer default ip address</b> command and the <b>member peer default ip address</b> command can be used to define default peer IP addresses.</li> </ul>



	Command or Action	Purpose
		<p><b>Note</b> 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.</p>
<b>Step 4</b>	<p><b>ip dhcp-server</b> [<i>ip-address</i>   <i>name</i>]</p> <p><b>Example:</b></p> <pre>Router(config)# ip dhcp-server 209.165.201.1</pre>	(Optional) Specifies the IP address of a DHCP server for the proxy client to use.
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Router(config)# end</pre>	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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<p><b>ip address-pool local</b></p> <p><b>Example:</b></p> <pre>Router(config)# ip address-pool local</pre>	Specifies local address pooling as the global default mechanism.

	Command or Action	Purpose
<b>Step 4</b>	<b>ip local pool</b> { <i>named-address-pool</i>   <b>default</b> } <i>first-IP-address</i> [ <i>last-IP-address</i> ] [ <b>group</b> <i>group-name</i> ] [ <b>cache-size</b> <i>size</i> ]  <b>Example:</b>  Router(config)# ip local pool default 192.0.2.1	Creates one or more local IP address pools.

## 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](#)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip dhcp-client network-discovery</b> <i>informs</i> <i>number-of-messages</i> <b>discovers</b> <i>number-of-messages</i> <b>period</b> <i>seconds</i>  <b>Example:</b>  Router(config)# ip dhcp-client network-discovery informs 2 discovers 2 period 2	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.

## 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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip local pool</b> { <i>named-address-pool</i>   <b>default</b> } { <i>first-IP-address</i> [ <i>last-IP-address</i> ]} [ <b>group</b> <i>group-name</i> ] [ <b>cache-size</b> <i>size</i> ] <b>Example:</b>  Router(config)# ip local pool default 192.0.2.0	Creates one or more local IP address pools.
<b>Step 4</b>	<b>interface</b> <i>type number</i> <b>Example:</b>  Router(config)# interface ethernet 2/0	Specifies the interface and enters interface configuration mode.
<b>Step 5</b>	<b>peer default ip address pool</b> <i>pool-name-list</i> <b>Example:</b>  Router(config-if)# peer default ip address pool 2	Specifies the pool or pools for the interface to use.
<b>Step 6</b>	<b>peer default ip address pool dhcp</b> <b>Example:</b>	Specifies DHCP as the IP address mechanism on this interface.

	Command or Action	Purpose
	Router(config-if)# peer default ip address pool dhcp	
<b>Step 7</b>	<b>peer default ip address ip-address</b> <b>Example:</b> Router(config-if)# peer default ip address 192.0.2.2	Specifies the IP address to assign to all dial-in peers on an interface.

## 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:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# configure terminal Enters global configuration mode.	
<b>Step 3</b>	<b>interface type number</b> <b>Example:</b> Router(config)# interface ethernet 0/1	Specifies the interface and enters interface configuration mode.
<b>Step 4</b>	<b>no peer neighbor-route</b> <b>Example:</b> Router(config-if)# no peer neighbor-route	Disables creation of neighbor routes.
<b>Step 5</b>	<b>peer neighbor-route</b> <b>Example:</b> Router(config-if)# peer neighbor-route	Reenables creation of neighbor routes.  <b>Note</b> If entered on a dialer or asynchronous group interface, this command affects all member interfaces.

## 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.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface serial <i>number</i></b> <b>Example:</b>  Router(config)# interface serial 0/0/1	Specifies an asynchronous interface and enters interface configuration mode.
<b>Step 4</b>	<b>no ip address</b> <b>Example:</b>  Router(config-if)# no ip address	Specifies no IP address for the interface.
<b>Step 5</b>	<b>encapsulation ppp</b> <b>Example:</b>	Enables PPP encapsulation.

	Command or Action	Purpose
	<code>Router(config-if)# encapsulation ppp</code>	
<b>Step 6</b>	<b>ppp multilink</b> <b>Example:</b> <code>Router(config-if)# ppp multilink</code>	Enables Multilink PPP.
<b>Step 7</b>	<b>pulse-time <i>seconds</i></b> <b>Example:</b> <code>Router(config-if)# pulse-time 60</code>	Enables pulsing data terminal ready (DTR) signal intervals on an interface.  <b>Note</b> 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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>interface multilink <i>group-number</i></b> <b>Example:</b> <code>Router(config)# interface multilink 2</code>	Creates a multilink bundle and enters interface configuration mode to configure the bundle.
<b>Step 4</b>	<b>ip address <i>address mask</i></b> <b>Example:</b> <code>Router(config-if)# ip address 192.0.2.1 255.255.255.224</code>	Sets a primary IP address for an interface.
<b>Step 5</b>	<b>encapsulation ppp</b> <b>Example:</b>	Enables PPP encapsulation.

	Command or Action	Purpose
	<code>Router(config-if)# encapsulation ppp</code>	
<b>Step 6</b>	<b>ppp chap hostname</b> <i>hostname</i> <b>Example:</b> <code>Router(config-if)# ppp chap hostname host1</code>	Specifies the hostname on the interface.
<b>Step 7</b>	<b>exit</b> <b>Example:</b> <code>Router(config-if)# exit</code>	Exits interface configuration mode.
<b>Step 8</b>	<b>interface</b> <i>type number</i> <b>Example:</b> <code>Router(config)# interface serial 0/0/1</code>	Enters interface configuration mode.
<b>Step 9</b>	<b>ppp multilink group</b> <i>group-number</i> <b>Example:</b> <code>Router(config-if)# ppp multilink group 2</code>	Restricts a physical link to joining only a designated multilink group interface.
<b>Step 10</b>	<b>exit</b> <b>Example:</b> <code>Router(config-if)# exit</code>	Exits interface configuration mode.

## Configuring PFC and ACFC

Protocol-Field-Compression (PFC) and Address-and-Control-Field-Compression (ACFC) 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

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <code>Router&gt; enable</code>	

	Command or Action	Purpose
	Enables privileged EXEC mode. Enter your password if prompted.	
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre> <p>Enters global configuration mode.</p>	
<b>Step 3</b>	<p><b>interface multilink <i>number</i></b></p> <p><b>Example:</b></p> <pre>Router(config)# interface multilink 2</pre>	Select a multilink interface.
<b>Step 4</b>	<p><b>ppp acfc local {request   forbid}</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# ppp acfc local request</pre>	<p>Configure how the router handles ACFC in its outbound configuration requests where:</p> <ul style="list-style-type: none"> <li>• <b>request</b>—The ACFC option is included in outbound configuration requests.</li> <li>• <b>forbid</b>—The ACFC option is not sent in outbound configuration requests, and requests from a remote peer to add the ACFC option are not accepted.</li> </ul>
<b>Step 5</b>	<p><b>ppp acfc remote {apply   reject   ignore}</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# ppp acfc remote apply</pre>	<p>Configure how the router handles the ACFC option in configuration requests received from a remote peer where:</p> <ul style="list-style-type: none"> <li>• <b>apply</b>—ACFC options are accepted and ACFC may be performed on frames sent to the remote peer.</li> <li>• <b>reject</b>—ACFC options are explicitly ignored.</li> <li>• <b>ignore</b>—ACFC options are accepted, but ACFC is not performed on frames sent to the remote peer.</li> </ul>
<b>Step 6</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# exit</pre>	Exits interface configuration mode.

**Configuring PFC**

Follow these steps to configure PFC handling during PPP negotiation:



## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre> Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>	
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface multilink <i>number</i></b> <b>Example:</b> <pre>Router(config)# interface multilink 2</pre>	Select a multilink interface.
<b>Step 4</b>	<b>ppp pfc local {request   forbid}</b> <b>Router(config-if)# ppp pfc local request</b>	Configure how the router handles PFC in its outbound configuration requests where: <ul style="list-style-type: none"> <li>• <b>request</b>—The PFC option is included in outbound configuration requests.</li> <li>• <b>forbid</b>—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted.</li> </ul>
<b>Step 5</b>	<b>ppp pfc remote {apply   reject   ignore}</b> <b>Example:</b> <pre>Router(config-if)# ppp pfc remote apply</pre>	Configure a method for the router to use to manage the PFC option in configuration requests received from a remote peer where: <ul style="list-style-type: none"> <li>• <b>apply</b>—PFC options are accepted and PFC may be performed on frames sent to the remote peer.</li> <li>• <b>reject</b>—PFC options are explicitly ignored.</li> <li>• <b>ignore</b>—PFC options are accepted, but PFC is not performed on frames sent to the remote peer.</li> </ul>
<b>Step 6</b>	<b>exit</b> <b>Example:</b> <pre>Router(config-if)# exit</pre>	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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface virtual template <i>number</i></b> <b>Example:</b> <pre>Router(config)# interface virtual template 1</pre>	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces and enters interface configuration mode.
<b>Step 4</b>	<b>ppp multilink endpoint {hostname   ip ipaddress   mac LAN-interface   none   phone telephone-number   string char-string}</b> <b>Example:</b> <pre>Router(config-if)# ppp multilink endpoint ip 192.0.2.0</pre>	Overrides or changes the default endpoint discriminator the system uses when negotiating the use of MLP with the peer.

## Creating a Multilink Bundle

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface multilink <i>group-number</i></b> <b>Example:</b>  Router(config)# interface multilink 10	Assigns a multilink group number and enters interface configuration mode.
<b>Step 4</b>	<b>ip address <i>address mask</i></b> <b>Example:</b>  Router(config-if)# ip address 192.0.2.9 255.255.255.224	Assigns an IP address to the multilink interface.
<b>Step 5</b>	<b>encapsulation ppp</b> <b>Example:</b>  Router(config-if)# encapsulation ppp	Enables PPP encapsulation.
<b>Step 6</b>	<b>ppp multilink</b> <b>Example:</b>  Router(config-if)# ppp multilink	Enables Multilink PPP.

## 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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>interface multilink</b> <i>group-number</i> <b>Example:</b>  Router(config)# interface multilink 10	Assigns a multilink group number and enters interface configuration mode.
<b>Step 4</b>	<b>no ip address</b> <b>Example:</b>  Router(config-if)# no ip address	Removes any specified IP address.
<b>Step 5</b>	<b>keepalive</b> <b>Example:</b>  Router(config-if)# keepalive	Sets the frequency of keepalive packets.
<b>Step 6</b>	<b>encapsulation ppp</b> <b>Example:</b>  Router(config-if)# encapsulation ppp	Enables PPP encapsulation.
<b>Step 7</b>	<b>ppp multilink group</b> <i>group-number</i> <b>Example:</b>  Router(config-if)# ppp multilink 12	Restricts a physical link to joining only the designated multilink-group interface.
<b>Step 8</b>	<b>ppp multilink</b> <b>Example:</b>  Router(config-if)# ppp multilink	Enables Multilink PPP.
<b>Step 9</b>	<b>ppp authentication chap</b> <b>Example:</b>  Router(config-if)# ppp authentication chap	(Optional) Enables CHAP authentication.
<b>Step 10</b>	<b>pulse-time</b> <i>seconds</i> <b>Example:</b>  Router(config-if)# pulse-time 10	(Optional) Configures DTR signal pulsing.

## 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.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface multilink <i>number</i></b> <b>Example:</b> <pre>Router(config)# interface multilink 10</pre>	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, and enters interface configuration mode.
<b>Step 4</b>	<b>ip address <i>ip-address mask</i></b> <b>Example:</b> <pre>Router(config-if)# ip address 10.13.1.1 255.255.255.0</pre>	Sets the IP address for the interface.
<b>Step 5</b>	<b>ppp multilink mrru [<i>local</i>   <i>remote</i>]</b> <i>mrru-value</i> <b>Example:</b> <pre>Router(config-if)# ppp multilink mrru local 1600</pre>	Configures the MRRU value negotiated on a multilink bundle when MLP is used. <ul style="list-style-type: none"> <li>• <b>local</b>—(Optional) Configures the local MRRU value. 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.</li> <li>• <b>remote</b>—(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.</li> </ul>
<b>Step 6</b>	<b>mtu bytes</b> <b>Example:</b> <pre>Router(config-if)# mtu 1600</pre>	(Optional) Adjusts the maximum packet size or MTU size. <ul style="list-style-type: none"> <li>• 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</li> </ul>

	Command or Action	Purpose
		<p>MLP frames, although it is not strictly necessary.</p> <ul style="list-style-type: none"> <li>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.</li> </ul>
<b>Step 7</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.
<b>Step 8</b>	<p><b>interface serial <i>slot/port</i></b></p> <p><b>Example:</b></p> <pre>Router(config)# interface serial 0/0</pre>	Selects a serial interface to configure and enters interface configuration mode.
<b>Step 9</b>	<p><b>ppp multilink</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# ppp multilink</pre>	Enables MLP on the interface.
<b>Step 10</b>	<p><b>ppp multilink group <i>group-number</i></b></p> <p><b>Example:</b></p> <pre>Router(config-if)# ppp multilink group 1</pre>	Restricts a physical link to joining only a designated multilink-group interface.
<b>Step 11</b>	<p><b>mtu <i>bytes</i></b></p> <p><b>Example:</b></p> <pre>Router(config-if)# mtu 1600</pre>	<p>(Optional) Adjusts the maximum packet size or MTU size.</p> <ul style="list-style-type: none"> <li>The default MTU for serial interfaces is 1500.</li> <li>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.</li> <li>You must ensure that fragmentation is performed such that fragments are sized less than the link interface MTU (refer to command pages for the <b>ppp multilink fragmentation</b> and <b>ppp multilink fragment-delay</b> commands for more</li> </ul>

	Command or Action	Purpose
		information about packet fragments), or configure the MTUs of the link interfaces such that they can transmit the larger frames.
<b>Step 12</b>	<b>exit</b> <b>Example:</b> <pre>Router(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.

## Disabling PPP Multilink Fragmentation

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface multilink <i>group-number</i></b> <b>Example:</b> <pre>Router(config)# interface multilink 10</pre>	Assigns a multilink group number and enters interface configuration mode.
<b>Step 4</b>	<b>ppp multilink fragment disable</b> <b>Example:</b> <pre>Router(config-if)# ppp multilink fragment disable</pre>	(Optional) Disables PPP multilink fragmentation.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> <pre>Router(config-if)# exit</pre>	Exits privileged EXEC mode.

### 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](#).





## CHAPTER 7

# Transparent SONET or SDH over Packet (TSoP) Protocol

**Table 6: Feature History**

Feature Name	Release Information	Description
SFP-TS-OC3STM1-I and SFP-TS-OC12STM4-I Optics Support	Cisco IOS XE 17.13.1	<p>SFP-TS-OC3STM1-I and SFP-TS-OC12STM4-I Optics Support is extended to the following chassis:</p> <ul style="list-style-type: none"> <li>• NCS 4201</li> <li>• NCS 4202</li> </ul> <p>These TSOP smart SFPs can operate in the low latency mode and is used for rail signaling.</p> <p><b>Note</b> The support for the ONS-SC-155-TSOP and ONS-SC-622-TSOP are deprecated and are replaced with the new TSoPs SFP-TS-OC3STM1-I and SFP-TS-OC12STM4-I optics, respectively. The software functionalities of the new TSoPs remain the same as the earlier TSoPs.</p>

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 146](#)
- [Restrictions for TSoP, on page 146](#)
- [Information About TSoP Smart SFP, on page 146](#)
- [Configuring the Reference Clock, on page 148](#)
- [Configuration Examples for TSoP, on page 149](#)
- [Verification Examples, on page 150](#)

## 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.
- 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 versa.

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.



- 
- Note** 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.



- 
- Note** 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 .
-

# 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).

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>interface type number</b> <b>Example:</b> Device(config)# <b>interface gigabitethernet 0/0/0</b>	Specifies the Gigabit Ethernet interface for configuration and enters interface configuration mode.
<b>Step 4</b>	<b>ssfpd tsop clock-source {ethernet   tdm}</b> <b>Example:</b> Device(config)# <b>ssfpd tsop clock-source ethernet</b>	Configures the reference clock on the interface. <ul style="list-style-type: none"> <li>• <b>ethernet</b>—Specifies the ethernet interface as clock source. Default is ethernet.</li> <li>• <b>tdm</b>—Specifies the TDM interface as clock source.</li> </ul> <p><b>Note</b> If Ethernet interface is selected as clock source, the TSoP Smart SFP is synchronized with the Ethernet interface's clock (where smart SFP is installed), which in turn is synchronized with the network clock (that is already chosen through PTP or SYNC-E).</p>

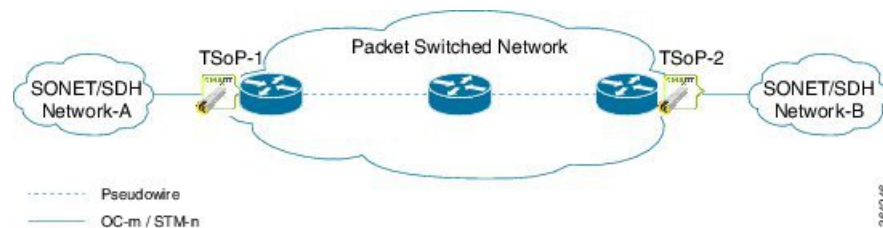
	Command or Action	Purpose
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config)# end	Exists configuration and enters privileged EXEC mode

## 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 Layer3 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 sspf-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

```

The following example shows the configuration of ASR-920-12CZ-D:

```

router#show platform
Chassis type: ASR-920-12CZ-D

```

Slot	Type	State	Insert time (ago)
0/0	12xGE-2x10GE-FIXED	ok	7w2d
R0	ASR-920-12CZ-D	ok, active	7w2d
F0		ok, active	7w2d
P0	ASR920-PSU0	ps, fail	never
P1	ASR920-PSU1	ok	never
P2	ASR920-FAN	ok	never

Slot	CPLD Version	Firmware Version
R0	20051844	15.6(53r)S
F0	20051844	15.6(53r)S

## Verifying Clock Source

- Use the **show platform software sspfd** 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
rtpSsrc: 0
```





## CHAPTER 8

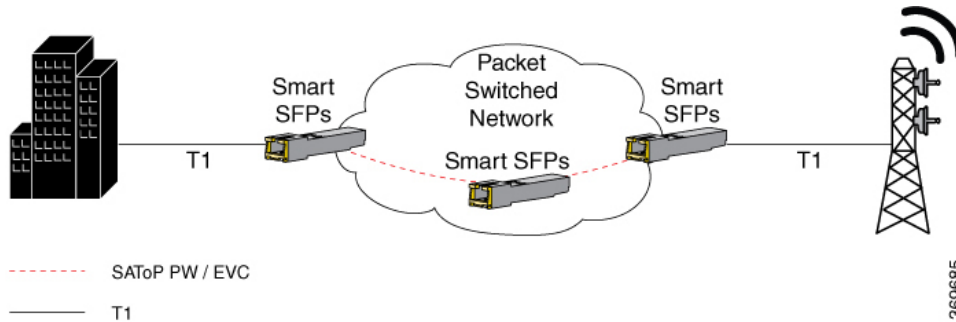
# Configuring TPoP Smart SFP

*Table 7: Feature History*

Feature Name	Release Information	Description
Support for T1 framed Smart TPoP pluggable	Cisco IOS XE Bengaluru 17.6.1	<p>You can configure the following features for T1 in framed mode:</p> <ul style="list-style-type: none"> <li>• Loopback, framing, line code encoding, cable length, and jitter buffer</li> <li>• BERT</li> <li>• Performance monitoring counters and alarms</li> <li>• Alarm profiling</li> <li>• Clock recovery modes</li> </ul> <p>These features that are configured on framed and unframed T1 interfaces help you to monitor the traffic and troubleshoot errors or failures efficiently.</p>
Support for E1 framed Smart TPoP pluggable	Cisco IOS XE Bengaluru 17.6.1	<p>You can configure the following features for E1 in framed and unframed modes:</p> <ul style="list-style-type: none"> <li>• Loopback, framing, line code encoding, cable length, and jitter buffer</li> <li>• BERT</li> <li>• Performance monitoring counters and alarms</li> <li>• Alarm profiling</li> <li>• Clock recovery modes</li> </ul> <p>These features that are configured on framed and unframed E1 interfaces help you to monitor the traffic and troubleshoot errors or failures efficiently.</p>

Transparent PDH over Packet (TPOp) Smart SFP is a special type of transceiver, which provides solution to encapsulate a T1 or E1 stream into a SAToP packet, suitable for pseudowire (PW) transport over a packet switched network (PSN).

**Figure 11: Network View with TPOp SSFPs**



The key component of TPOp is the interworking function that provides packetization, depacketization, and clock recovery that translate the TDM bit stream to a packet stream, and conversely. TPOp approach is similar to the SAToP method, where the entire T1 or E1 is encapsulated in a single circuit emulating pseudowire and transport it to a single destination over the PSN.

- [Features of TPOp Smart SFP, on page 154](#)
- [TPOp Prerequisites, on page 155](#)
- [Restrictions for TPOp Smart SFP, on page 156](#)
- [How to Configure TPOp Smart SFP, on page 156](#)

## Features of TPOp Smart SFP

The TPOp smart SFP supports the following Cisco ASR 920 series routers:

- NCS4201-SA
- NCS4202-SA

The TPOp smart SFP supports the following features:

- Unframed SAToP support on the below optics:
  - ONS-SI-DS1-TPOP
- Starting with Cisco IOS XE Bengaluru 17.6.1, framed SAToP is supported on the below optics:
  - SFP-T1F-SATOP-I
  - SFP-E1F-SATOP-I
- Supports local and network loopback.
- Supports Interworking Functionality (IWF) Performance Monitoring (PM) counters.
- Supports the following alarms for T1, E1, :
  - T1 unframed—Loss of Signal (LOS)

- T1 framed—LOS, Loss of Frame (LOF), Remote Alarm Indication (RAI), and Alarm Indication Signal (AIS)
- E1 framed—LOS, LOF, RAI, and AIS
- Supports the clock recovery modes such as Adaptive Clock Recovery (ACR), Differential Clock Recovery (DCR), or retiming mode.




---

**Note** Retiming mode is the default mode (Using common clock source through SYNCE or same external source for PE nodes)

---

- Supports cable length and jitter buffer.
- Peer end side of the TPoP smart SFP could be TPoP smart SFP or IM that supports the SAToP protocol.
- Supports BERT, line encoding, and performance monitoring on the below optics:
  - SFP-T1F-SATOP-I
  - SFP-E1F-SATOP-I

## TPoP Prerequisites

- The Multiprotocol Label Switching (MPLS) and Interior Gateway Protocol (IGP) endpoints are up and running fine between the PE nodes.
- Use either one of the following modes for node synchronization:
  - Ensure that SyncE is configured.
  - Use the PTP Telecom profile, G.8265.1 for frequency synchronization, for CEM.
  - If SyncE and PTP Telecom profile/G.8265.1 for frequency synchronization are not supported for CEM, then use ACR to time TPoP CEM psedowires.
- Port interface should be set as default using the **default int Gig 0/0/8** command before inserting TPoP smart SFP on GE or 10GE port.
- The GE or 10GE port interface is brought up using the **no shutdown** command.
- In cases where a non-TPoP SFP is to be inserted on any port from which any TPoP smart SFP is removed, then before inserting non-TPoP SFP, the TPoP smart SFP configuration is removed using the following commands:
  - For T1
    - no platform smart-sfp interface Gig x/y/z type t1**
    - no platform smart-sfp interface TenGig x/y/z type t1**
  - For T1 Framed
    - no platform smart-sfp interface Gig x/y/z type t1-framed**

- For E1 Framed

**no platform smart-sfp interface Gig x/y/z type e1-framed**




---

**Note** Recovered clock configuration needs to be removed before applying the **no platform** command.

---

## Restrictions for TPOp Smart SFP

- The payload for T1 is limited to 192 bytes, and for T3 is limited to 1024 bytes.
- It's observed that the ACR and DCR clock status may change from **locked** state to **acquiring** state, and the opposite way. This is the expected behavior and doesn't have any impact on functionality.
- Framed SAToP and CESoP aren't supported on ONS-SI-DS1-TPOP.
- CESoP isn't supported in framed T1, E1, or T3.
- BERT and BERT statistics aren't supported on ONS-SI-DS1-TPOP.
- Error insertion in BERT isn't supported.
- PMON counters aren't supported on ONS-SI-DS1-TPOP.
- The Cisco ASR-920-24SZ-M router supports a maximum of 8 TPOp smartSFPs and only on any of the 12 GE ports of the top row, which has odd-numbered ports.
- The Cisco ASR-920-12SZ-IM router supports a maximum of eight TPOp smart SFPs on four GE and four 10GE ports.
- Remote loopback isn't supported.

## How to Configure TPOp Smart SFP

### Enabling TPOp Smart SFP

To enable TPOp smart SFP on the unframed T1 mode, enter the following commands:

```
Router# configure terminal
Router(config)# platform smart-sfp interface gig slot/bay/port type T1
Router(config)# exit
```

To enable TPOp smart SFP on the T1 framed mode, enter the following commands:

```
Router# configure terminal
Router(config)# platform smart-sfp interface gig slot/bay/port type T1-FRAMED
Router(config)# exit
```

To enable TPOp smart SFP on the E1 framed mode, enter the following commands:

```
Router# configure terminal
Router(config)# platform smart-sfp interface gig slot/bay/port type E1-FRAMED
Router(config)# exit
```

## Configuring CEM Circuits

To configure CEM circuits on unframed T1 TPOp, enter the following commands:

```
enable
configure terminal
controller t1 0/0/10
cem-group 0 unframed
end
```

To configure CEM circuits on framed T1 TPOp, enter the following commands:

```
enable
configure terminal
controller t1 0/0/10
cem-group 0 framed
end
```

To configure CEM circuits on unframed E1 TPOp, enter the following commands:

```
enable
configure terminal
controller e1 0/0/10
cem-group 0 unframed
end
```

To configure CEM circuits on framed E1 TPOp, enter the following commands:

```
enable
configure terminal
controller e1 0/0/10
cem-group 0 framed
end
```

## Configuring Cable Length

You can configure a cable length (in feet) on the unframed T1 mode for releases before Cisco IOS XE Bengaluru 17.6.1. Starting with Cisco IOS XE Bengaluru 17.6.1, you can configure the cable length on the framed T1 mode.



---

**Note** Cable length is not supported on the E1 TPOp smart SFP.

---

- You can configure the cable length in one of the following five ranges:

**Table 8: Cable Length Values for T1 - SFP-T1F-SATOP-I, SFP-E1F-SATOP-I, ONS-SI-DS1-TPOP**

Cable Length (in ft)	Range (in ft)
110	0–133
220	134–266
330	267–399
440	400–533
550	534–655

To configure the cable length on the unframed and framed T1 modes for TPoP smart SFP, enter the following commands:

```
enable
configure terminal
controller t1 x/y/z
cablelength short <value>
end
```

To configure a cable length of 266 feet on the t1 0/0/0 interface, enter the following commands:

```
enable
configure terminal
controller t1 0/0/10
cablelength short 266
end
```

## Configuring Linecode

You can configure linecode encoding on unframed or framed T1 and E1 modes for TPoP smart SFPs.

The TPoP smart SFPs support the following linecode encoding for framed T1 and E1 modes:

- T1 framed SFP—AMI or B8ZS
- E1 framed SFP—HDB3 or AMI

To configure linecode on T1 controller, enter the following commands:

```
router#controller t1 0/0/1
router(config-controller)#linecode {ami | b8zs}
router(config-controller)#end
```

To configure linecode on E1 controller, enter the following commands:

```
router#controller e1 0/0/7
router(config-controller)#linecode {ami | hdb3}
```

```
router(config-controller)#end
```

The following example on how to configure AMI linecode encoding on T1 controller for TPOp:

```
router#controller t1 0/0/1
router(config-controller)#linecode ami
router(config-controller)#end
```

## Configuring Dejitte Buffer and Payload

You can configure jitter buffer on unframed T1 for releases prior to Cisco IOS XE Bengaluru 17.6.1. Starting with Cisco IOS XE Bengaluru 17.6.1, you can configure jitter buffer on framed T1, unframed, and framed E1 for TPOp Smart SFP. You can configure a maximum jitter buffer value from 3 through 32 ms.

To configure jitter buffer, enter the following commands:

```
router#interface cem0/0/11
router(config-if)#cem 0
router#dejitter-buffer 5
```

You can configure a payload with size of 192 bytes for T1, 256 bytes for E1.

To configure the payload, enter the following commands:

```
router#interface cem0/0/11
router#cem 0
router#payload-size 192
```

## Configuring BERT

You can configure BERT on unframed and framed T1 and E1 for TPOp smart SFPs.

To configure BERT on T1 controller, enter the following commands:

```
router(config)#controller t1 0/0/1
router(config-controller)#bert pattern PRBS interval 1 direction line
router(config-controller)#end
```

The PRBS pattern range for T1 controller is non-inverted 2<sup>15</sup>-1 O.151 test pattern and the default pattern for E1 is inverted 2<sup>15</sup>-1 .

To configure BERT on E1 controller, enter the following commands:

```
router(config)#controller e1 0/0/3
router(config-controller)#bert pattern PRBS interval 1 direction line
router(config-controller)#end
```

To configure system BERT on T1 controller in the unframed mode, enter the following commands:

```
router(config)#controller t1 0/0/17
```

```
router(config-controller)#bert pattern PRBS interval 1 direction system
router(config-controller)#end
```

To configure system BERT on E1 controller in the unframed mode, enter the following commands:

```
router(config)#controller e1 0/0/17
router(config-controller)#bert pattern PRBS interval 1 direction system
router(config-controller)#end
```




---

**Note** The system side BERT is supported only on unframed mode and is not supported with ESF or SF framing. The line side BERT is supported for all framing types.

---

## Loopback on TPoP Smart SFP

TPoP smart SFP supports two types of loopback configurations:

- Local loopback—In a local loopback, the transmitting signal loops back to the receiver signal.
- Network loopback—In a network loopback, the receiving signal loops back to the transmitting signal.

## Configuring Loopback on TPoP

### Configuring Network Loopback

Follow these steps to configure a network loopback on T1 for TPoP:

```
enable
configure terminal
controller t1 x/y/z
loopback network line
exit
```

### Configuring Local Loopback

Follow these steps to configure a local loopback on T1 for TPoP:

```
enable
configure terminal
controller t1 x/y/z
loopback local
exit
```

The following example explains on how to configure the network loopback on T1 for TPoP:

```
Router(config)#controller t1 0/0/4
Router(config-controller)#loopback network line
```

The following example explains on how to configure the local loopback on T1 for TPoP:

```
Router(config)#controller t3 0/0/4
Router(config-controller)#loopback local
```



## Verifying Loopback at Controller Level

Use the **show controller t1 x/y/z** command to verify the local loopback configuration on T1 controller for TPOp smart SFP.

```
Router#show controllers T1 0/0/4
T1 0/0/4 is up (Local Loopback)
  Applique type is 2xGE-4x10GE-FIXED
  Cablelength is short 133
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Framing is unframed, Line Code is B8ZS, Clock Source is Internal.
  BER thresholds:  SF = 10e-3  SD = 10e-6
  Data in current interval (0 seconds elapsed):
    Near End
      0 Line Code Violations, 0 Path Code Violations
      0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
      0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
      0 Path Failures, 0 SEF/AIS Secs
    Far End
      0 Line Code Violations, 0 Path Code Violations
      0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
      0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
      0 Path Failures
```

Use the **show controller t1 x/y/z** command to verify the network loopback configuration on TPOp smart SFP.

```
router#show controller T1 0/0/4
T1 0/0/4 is up (Network Line Loopback)
  Applique type is 2xGE-4x10GE-FIXED
  Cablelength is short 133
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Framing is unframed, Line Code is B8ZS, Clock Source is Internal.
  BER thresholds:  SF = 10e-3  SD = 10e-6
  Data in current interval (0 seconds elapsed):
    Near End
      0 Line Code Violations, 0 Path Code Violations
      0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
      0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
      0 Path Failures, 0 SEF/AIS Secs
    Far End
      0 Line Code Violations, 0 Path Code Violations
      0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
      0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
      0 Path Failures
```

Use the **show controller t1 x/y/z** command to verify the local loopback configuration for framed T1 mode on TPOp smart SFP.

```
router#show controller t1 0/0/1
T1 0/0/1 is up (Local Loopback)
  Applique type is 24xGE-4x10GE-FIXED-S
  Cablelength is short 133
  Receiver has no alarms.
  alarm-trigger is not set
```

```

Soaking time: 3, Clearance time: 10
Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
BER thresholds: SF = 10e-3 SD = 10e-6
Data in current interval (0 seconds elapsed):
Near End
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  0 Path Failures, 1 SEF/AIS Secs
Far End
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  0 Path Failures

```

Use the **show controller t1 x/y/z** command to verify the network loopback configuration for framed T1 mode on TPoP smart SFP.

```

router#show controller t1 0/0/1
T1 0/0/1 is up (Network Line Loopback)
  Applique type is 24xGE-4x10GE-FIXED-S
  Cablelength is short 133
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
  BER thresholds: SF = 10e-3 SD = 10e-6
  Data in current interval (0 seconds elapsed):
  Near End
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
    0 Path Failures, 2 SEF/AIS Secs
  Far End
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
    0 Path Failures

```

Use the **show controller e1 x/y/z** command to verify the local loopback configuration for E1 framed mode on TPoP smart SFP.

```

router#show controllers e1 0/0/12
E1 0/0/12 is up (Local Loopback)
  Applique type is 12xGE-4x10GE-FIXED
  Cablelength is Unknown
  Receiver has no alarms.
  alarm-trigger is not set
  Framing is crc4, Line Code is HDB3, Clock Source is Internal.
  BER thresholds: SF = 10e-5 SD = 10e-5
  Data in current interval (80 seconds elapsed):
  Near End
    495 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 1 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 79 Unavail Secs
    1 Path Failures, 0 SEF/AIS Secs
  Far End
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 79 Unavail Secs
    1 Path Failures

```

Use the **show controller e1 x/y/z** command to verify the local loopback configuration for E1 unframed mode on TPOp smart SFP.

```
router#show controllers e1 0/0/12
E1 0/0/17 is up (Local Loopback)
Applique type is 24xGE-4x10GE-FIXED-S
Cablelength is Unknown
No alarms detected.
alarm-trigger is not set
Framing is unframed, Line Code is HDB3, Clock Source is Internal.
BER thresholds: SF = 10e-5 SD = 10e-5
Data in current interval (0 seconds elapsed):
Near End
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
0 Path Failures, 0 SEF/AIS Secs
Far End
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
0 Path Failures
```

## Performance Monitoring on TPOp

You can view the statistics or error count generated on the TPOp SFP.

The TPOp Smart SFP in the T1 or E1 framed mode supports the following counters to monitor the performance.

- Line Code Violation (LCV)
- Path Code Violation (PCV)

For T1 and E1 links, the Loss of Frame (LOF) failure is declared when an OOF defect is detected. Based on OOF and other alarms, the below existing counters and their far-end counters are calculated.

- Framed Loss Seconds (SELS)
- Line Errored Seconds (LES)
- Errored Seconds (ES)
- Severely Errored Seconds (SES)
- Unavailable Seconds (UAS)
- Errored Seconds Far End (ES-FE)
- Severely Errored Seconds in Far End (SES-FE)
- Unavailable Seconds in Far End (UAS-FE)
- AIS Seconds (AISS/SEF)
- Failure Count at Path (FCP)




---

**Note** Far-end counters are supported only in ESF framing mode and not supported in unframed and SF modes.

---

To view the statistics or error count generated, use the **show controller t1** command:

```
router#show controller t1 0/0/1
T1 0/0/1 is up
  Applique type is 24xGE-4x10GE-FIXED-S
  Cablelength is short 133
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
  BER thresholds: SF = 10e-3 SD = 10e-6
  Data in current interval (0 seconds elapsed):
    Near End
      0 Line Code Violations, 0 Path Code Violations
      0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
      0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
      0 Path Failures, 0 SEF/AIS Secs
    Far End
      0 Line Code Violations, 0 Path Code Violations
      0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
      0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
      0 Path Failures
```

## Configuring Clocking Recovery System for TPoP

### Adaptive Clock Recovery

Adaptive Clock Recovery (ACR) is an averaging process that negates the effect of random packet delay variation and captures the average rate of transmission of the original bit stream. ACR recovers the original clock for a synchronous data stream from the actual payload of the data stream.

For more information, see [Adaptive Clock Recovery](#).

### Differential Clock Recovery

Differential Clock Recovery (DCR) is another technique that is used for Circuit Emulation (CEM) to recover clocks based on the difference between PE clocks.

For more information, see [Differential Clock Recovery](#).

## Prerequisites for Clock Recovery

- You must configure CEM before configuring the global clock recovery.
- RTP is enabled by default for DCR in CEM. If DCR configuration is removed, then you must remove the RTP configuration manually under CEM.

## Configuring ACR

To configure the clock for TPoP in the T1 controller mode, use the following commands:

```
enable
configure terminal
controller t1 0/0/1
clock source recovered 1
cem-group 0 unframed
exit
```

```
enable
configure terminal
controller t1 0/0/1
clock source recovered 1
cem-group 0 framed
exit
```

To configure the clock for TPOp in the E1 controller mode, use the following commands:

```
enable
configure terminal
controller e1 0/0/1
clock source recovered 1
cem-group 0 framed
exit
```

```
enable
configure terminal
controller e1 0/0/1
clock source recovered 1
cem-group 0 unframed
exit
```




---

**Note** For ACR mode: Wander compliant to ITU-T G.823/G.824 for traffic interfaces, and MEF18. The Wander Performance is only validated and measured according to ITU-T G.8261 test case TC1, performance for other test cases and PDV impairments is not tested or guaranteed.

---

To configure the clock recovery in global configuration mode, use the following commands:

```
recovered-clock 0 0
clock recovered 1 adaptive cem 1 0
exit
```

## Verifying ACR Configuration for TPOp

Use the **show recovered-clock** command to verify the adaptive clock recovery of T1 interfaces for TPOp:

```
Router#show recovered-clock
Recovered clock status for subslot 0/0
-----
Clock   Type      AUG-MAP  Mode      CEM   Status      Frequency  Offset (ppb)  Circuit-No
-----
1       T1        NA       ADAPTIVE  0     ACQUIRED    NA         NA            1 (Port)
      Priority
      NA
```




---

**Note** Starting with release Cisco IOS XE Cupertino 17.9.1, TPOp T1/E1 clock status is accurately displayed in the recovered clock status output.

---

Use the **show running-config** command to verify the configuration of adaptive clock of T1 interfaces:

```
Router# show running-config | section x/y/z
```

```

controller T1 x/y/z
threshold sd-ber 6
threshold sf-ber 3
framing esf
clock source recovered 1
linecode b8zs
cablelength short 110
cem-group 0 framed
interface CEM x/y/z
no ip address
cem 0
!
```

```

Router#show running-config | sec 0/0/1
platform smart-sfp interface GigabitEthernet0/0/1 type T1-FRAMED
controller T1 0/0/1
  threshold sd-ber 6
  threshold sf-ber 3
  framing esf
  clock source recovered 1
  linecode b8zs
  cem-group 0 framed
interface CEM0/0/1
  no ip address
  cem 0
  xconnect 2.2.2.2 1 encapsulation mpls
```

Use the **show running-config | section recovered-clock** command to verify the recovery of adaptive clock of T1 interfaces:

```

Router# show running-config | section recovered-clock
recovered-clock 0 0
  clock recovered 1 adaptive cem 1 0
```

## Configuring DCR

To configure the clock for TPoP in the T1 controller mode, use the following commands:

```

enable
configure terminal
controller t1 0/0/1
clock source recovered 1
cem-group 0 unframed
exit
```

```

enable
configure terminal
controller t1 0/0/1
clock source recovered 1
cem-group 0 framed
exit
```

To configure the clock for TPoP in the E1 controller mode, use the following commands:

```

enable
configure terminal
controller e1 0/0/1
```

```
clock source recovered 1
cem-group 0 unframed
exit
```

```
enable
configure terminal
controller e1 0/0/1
clock source recovered 1
cem-group 0 framed
exit
```

The **rtp-present** is added by default, when DCR is configured.

To configure RTP header in global configuration mode, use the following commands:

```
interface cem 0/0/1
cem 0
rtp-present
```

To configure differential clock recovery, use the following commands in global configuration mode:

```
recovered-clock 0 0
clock recovered 1 differential cem 1 0
exit
```

## Verifying DCR Configuration for TPOp

Use the **show recovered-clock** command to verify the differential clock recovery of T1 interfaces for TPOp:

```
Router#show recovered-clock
Recovered clock status for subslot 0/0
-----
Clock      Type      AUG-MAP  Mode          CEM  Status  Frequency Offset (ppb)  Circuit-No
          Priority
1          T1        NA       DIFFERENTIAL 0    NA      NA          1 (Port)
          NA
```



**Note** There is a hardware limitation to display the status of the clock. The **show recovered-clock** command is just an indication for the configured recovered clock.

Use the **show running-config | section** command to verify the configuration of differential clock of T1 interfaces for TPOp:

```
Router# show running-config | section 0/0/1
controller T1 x/y/z
 framing unframed
 clock source recovered 1
 linecode b8zs
 cablelength long 0db
  cem-group 0 unframed
interface CEM x/y/z
 no ip address
 cem 0
 rtp-present
```

```
Router#show running-config | sec 0/0/1
platform smart-sfp interface GigabitEthernet0/0/1 type T1-FRAMED
controller T1 0/0/1
  threshold sd-ber 6
  threshold sf-ber 3
  framing esf
  clock source recovered 1
  linecode b8zs
  cem-group 0 framed
interface CEM0/0/1
  no ip address
  cem 0
  rtp-present
  xconnect 2.2.2.2 1 encapsulation mpls
!
```

Use the **show running-config | section recovered-clock** command to verify the recovery of differential clock of T1 interfaces:

```
Router# show running-config | section recovered-clock
recovered-clock 0 0
  clock recovered 1 differential cem 1 0
```

Use the **show running-config | section** command to verify the configuration of differential clock of T1 interfaces for TPoP:

```
Router# show running-config | section 0/0/1
controller T1 x/y/z
  framing unframed
  clock source recovered 1
  linecode b8zs
  cablelength long 0db
  cem-group 0 unframed
interface CEM x/y/z
  no ip address
  cem 0
  rtp-present
```

## Verifying TPoP Smart SFP Configuration

Use the following show commands to verify the TPoP smart SFP configuration:

- **show controller {t1} slot/subslot/port**—Displays the TPoP Smart SFP information available in the slot/subslot/port, if any, along with the other controllers information. T1 specifies the TPoP T1 specific controller.
  - show cem cir id**—Displays the CEM circuit statistics or configuration.
- **show controller {e1} slot/subslot/port**—Displays the TPoP Smart SFP information available in the slot/subslot/port, if any, along with the other controllers information. E1 specifies the TPoP T1 specific controller.
  - show cem cir id**—Displays the CEM circuit statistics or configuration.

```
router#show controller t1 0/0/4
T1 0/0/4 is up (Network Line Loopback)
```



```

Applique type is 2xGE-4x10GE-FIXED
Cablelength is short 133
No alarms detected.
alarm-trigger is not set
Soaking time: 3, Clearance time: 10
AIS State:Clear LOS State:Clear LOF State:Clear
Framing is unframed, Line Code is B8ZS, Clock Source is Internal.
BER thresholds: SF = 10e-3 SD = 10e-6
Data in current interval (0 seconds elapsed):
Near End
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  0 Path Failures, 0 SEF/AIS Secs
Far End
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  0 Path Failures

```

```

router#show controller e1 0/0/17
E1 0/0/17 is up
Applique type is 24xGE-4x10GE-FIXED-S
Cablelength is Unknown
No alarms detected.
alarm-trigger is not set
Framing is crc4, Line Code is HDB3, Clock Source is Internal.
BER thresholds: SF = 10e-5 SD = 10e-5
Data in current interval (190 seconds elapsed):
Near End
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  0 Path Failures, 0 SEF/AIS Secs
Far End
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  1 Errored Secs, 0 Bursty Err Secs, 1 Severely Err Secs, 0 Unavail Secs
  0 Path Failures

```

```

router#show controller e1 0/0/12
E1 0/0/12 is up (Local Loopback)
Applique type is 12xGE-4x10GE-FIXED
Cablelength is Unknown
Receiver has no alarms.
alarm-trigger is not set
Framing is crc4, Line Code is HDB3, Clock Source is Internal.
BER thresholds: SF = 10e-5 SD = 10e-5
Data in current interval (750 seconds elapsed):
Near End
  14 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 2 Fr Loss Secs, 2 Line Err Secs, 0 Degraded Mins
  2 Errored Secs, 0 Bursty Err Secs, 2 Severely Err Secs, 0 Unavail Secs
  0 Path Failures, 2 SEF/AIS Secs
Far End
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  0 Path Failures

```

```

Router#show cem cir int CEM 0/0/4

```

```
CEM0/0/4, ID: 0, Line: UP, Admin: UP, Ckt: ACTIVE
Mode :T1, CEM Mode: T1-SAToP
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:      8273275          Dropped:           0
Egress Pkts:       8273275          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          Severly Errored Sec: 0
Unavailable Sec:   0          Failure Counts:     0
Pkts Malformed:   0          JitterBuf Overrun:  0
```

## Router#show cem circuit int CEM 0/0/1

```
CEM0/0/1, ID: 0, Line: UP, Admin: UP, Ckt: ACTIVE
Mode :T1, CEM Mode: T1-SAToP
Controller state: up, T1/E1 state: up
Idle Pattern: 0xFF, Idle CAS: 0x8 0x8
Dejitter: 5 (In use: 0)
Payload Size: 192
Framing: Framed SAToP
CEM Defects Set
None
```

```
Signalling: No CAS
RTP: Configured, RTP-HDR Compression: Disabled
```

```
Ingress Pkts:      122663          Dropped:           0
Egress Pkts:       122663          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          Severly Errored Sec: 0
Unavailable Sec:   0          Failure Counts:     0
Pkts Malformed:   0          JitterBuf Overrun:  0
```

## router#show cem circuit 0

```
CEM0/0/12, ID: 0, Line: UP, Admin: UP, Ckt: ACTIVE
Mode :E1, CEM Mode: E1-SAToP
Controller state: up, T1/E1 state: up
Idle Pattern: 0xFF, Idle CAS: 0x8 0x8
Dejitter: 5 (In use: 0)
Payload Size: 256
Framing: Framed SAToP
CEM Defects Set
None
```

```
Signalling: No CAS
RTP: No RTP

Ingress Pkts: 6000 Dropped: 0

Egress Pkts: 6000 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 Severly Errored Sec: 0

Unavailable Sec: 0 Failure Counts: 0

Pkts Malformed: 0 JitterBuf Overrun: 0
```

