Transparent PDH over Packet (TPoP) and Channelized SDH over Packet (CSoP)

Transparent PDH over Packet (TPoP) Smart SFP converts E1 traffic to a packet stream using TDM over packet pseudo-wire technology. TPoP Smart SFP can be used on selected SFP slots in a router to transport PDH traffic across a packet network. TPoP Smart SFP is a plug-and-play device which can be used without any provisioning and simplifies configuration and service turn-up of E1 connections across a packet network. The integration of TPoP into an SFP greatly reduces system and network complexity, offers lower carbon footprint, and results in savings.

Channelized SDH over Packet (CSoP) Smart SFP converts a fully channelized SDH signal to a packet stream using TDM over packet pseudo-wire technology. CSoP Smart SFP can replace an existing SFP in a router or a switch and transport E1 traffic across a packet network. CSoP Smart SFP aggregates single E1 and enables each E1 channel to be processed individually to provide a high-density gateway between an SDH network and a TDM over packet ethernet or IP or MPLS network.

Following are the supported E1 and STM1 optical SFPs, for more information on the supported router variants based on the release versions, see Cisco Optics-to-Device Compatibility Matrix.

- Framed STM1-ch E1 type: SFP-CH-OC3STM1-I
- Framed PDH E1 type: SFP-E1F-SATOP-I
- Clear channel STM1 type: SFP-TS-OC3STM1-I

Restrictions for Smart SFP

Warning If MR-APS is configured on the SFP, then remove MR-APS configuration before you remove the SFP from the port.

- CEM interface configuration isn’t supported.
- The following default attributes are available only under CEM interface configuration. But you can't configure these attributes, as the configuration CLIs aren’t supported.
    - dummy mode
    - dummy pattern
    - idle pattern
- E1 emulation is supported only on Ethernet pseudowire (VPWS).
- CSoP doesn’t support E1-AIS alarm.
- No support to Single Router–Automatic Protection Switching (SR-APS)
- CLI configuration for the E1 controller on a VLAN needs to be mapped to an Ethernet sub-interface (by configuring same VLAN dot1q under the sub-interface). Any xconnect, also must be configured with this ethernet sub-interface.
- Multi Router-Automatic Protection Switching (MR-APS) is supported only by using the VLAN PW.
- Ensure that you have more than one MPLS paths, in core to convergence during core failure scenario.
- Only 8 smart SFPs are supported per router.
- ACR clocking is not supported in TPoP and CSoP unframed SFPs. Only framed to framed connection is supported, so not supported on framed to unframed connections.
- STM1 CSoP:
    - E1 Level shutdown is not supported.
    - Controller shutdown won’t inject AIS but injects only LOS towards CE.
    - Bit error rate test (BERT) can be run only on one E1 channelized controller.
- CSoP and TPoP:
    - 25G ports are not supported.
    - Bit error rate is not supported.
- SF or SD threshold is not supported.
- Only 16-byte J0 is supported.
- BERT is not supported in unframed SFP.
- Loopback is supported only on, one of the 63 channels of CSoP SFP.
- Configuration with same ECID for CSoP E1s is not supported. ECID must be unique for each E1 under CSoP.
- The **show alarm conditions** command is not supported in Release 7.5.1.
- High convergence of 100ms is observed for MR-APS for LOS based switchover (for CSoP E1s).

- With smart SFP, high convergence of 4-6 minutes is observed in MR-APS for router reload based switchover.
- CSoP loopback on framed STM1-ch E1 doesn't work over **reload warm** command with smart SFP. Applicable only in Release 7.5.1.
- FPD upgrade for smart SFP is supported only from Release 7.8.1.
- LCV counter updates are not supported for smart SFP.
- In Cisco IOS XR software version 25.2.1, the N540X-16Z4G8Q2C-A and N540X-16Z4G8Q2C-D does not suppot Smart SFPs.

Configuring TPoP and CSoP

Consider a deployment scenario with the TDM circuits from a base transceiver station is connected to an access router and must be transported to the base station controller through an aggregation router over an MPLS network through pseudowire.

During aggregation from transceiver to controller, the TDM circuits protect the data by using smart SFPs. For the E1 lines coming from transceiver, you must use TPoP SFPs and for the STM-1 lines coming from transceiver or controller, you must use CSoP SFPs.

You can monitor the alarms and performances on TPoP and CSoP smart SFPs.

Table 1: Support on E1 Transmission

Feature	E1 Framed
SATOP	Supported
Clock configuration	ACR, DCR, internal, Line
BERT - System/Line	Supported (Inverted-PRBS15)
PM -E1	SELS, LES, UAS, LCV, PCV Far End counters are NOT SUPPORTED
Alarms	LOS, AIS, LOF, RDI
Loopback - (local / line)	Supported
CEM counters	Supported

Table 2: Support on OC3-STM1 Transmission

Feature	OC3-STM1
E1 SATOP	STM-1 Channelized E1
Clock Configuration on Channelised-E1	ACR, DCR, internal, Line
E1 Channel BERT - System/Line channel prbs	Supported (Inverted-PRBS15)

Feature	OC3-STM1
PM-STM1 RS/MS	ES, SES, UAS Far End counters are NOT SUPPORTED
Threshold and its alerts	Supported
Alarms STM1	LOS, LOF, RS-TIM, MS-AIS, MS-RAI

Also consider a case, with Automatic Protection Switching (APS) protection being enabled on the controller, then the protect link coming from a single node or from multiple nodes with standby pseudowire is supported in the MPLS core.

Configuring Controller for PDH E1

To configure PDH E1 on a controller, ensure the Gigabit Ethernet port is up and enter the following commands:

```
enable
configure terminal
    controller e1  0/0/0/7
    vlan 100 ecid 1
end
```

You must mention a unique VLAN ID which is specific to that port and ecid number to identify E1.

Verifying Controller for PDH E1

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

```
Router# show controller e1 0/0/0/7
Controller State: Up
Transport Admin State: In Service
Framing: Unframed
Linecoding: High Density Bipolar Order 3
Loopback: None
Clock: Adaptive Clock Recovery (ACR)
Clock State: Locked
VLAN ID: 100
ecid:1
```

Configuring Controller for STM1

To configure STM1 on a controller, ensure the Gigabit Ethernet port is up and enter the following commands:

```
controller STM1 0/0/0/18
 aug-mapping au4 au-4 1
  mode tug3
   tug-3 1
    mode tug2
     tug-2 1 payload vc12
      vc12 1 mapping e1

/*Configure STM1-ch E1 */
```

Verifying Controller for STM1

Use the **show controller stm1 x/y/z** command to verify the controller configuration on STM1 for CSoP smart SFP.

```
Router# show controller STM1 0/0/0/18
Port STM 10/0/0/18

Status:
Primary State: Up
Configured Sec admin State: Normal
Inherited Sec admin State: Normal
Derived State: In Service
performance_monitoring_enabled
Loopback: None
```

Configuring Controller for STM1-ch E1

To configure each E1 on STM1 port, enter the following commands:

```
Config terminal
    controller E1 0/0/0/18/1/1/1/1
    vlan 200 ecid 1
```

You can configure the same VLAN ID for all the E1 under the same STM1 port or a different VLAN ID for each E1 under that STM1 port.

Verifying Controller for STM1-ch E1

Use the **show controller e1 x/y/z** command to verify the controller configuration on STM1.

```
Router# show controller e1 0/0/0/18/1/1/1/1
Controller State: Up
Transport Admin State: In Service
Framing: Unframed
Linecoding: None
Loopback: None
Clock: Internal

VLAN ID: 200
ecid:1
```

VPWS with Smart SFP

The TDM circuits flows through the VPWS with smart SFP packetizing the incoming TDM frames. Packetizing happens with the following process:

- All frames from the TDM lines are channelized until E1 and then packetized.
- The packetization is done by adding:
    - RTP header – For DCR clocking support
    - VLAN header – For uniquely identifying the E1 channel
    - ENET header – The Ethernet DMAC and SMAC
    - CW – control word for communicating the sequence number, faults in the access side
    - Payload – the incoming TDM frames are chopped into 193Bytes frames and added into the payload.
    - The packets mentioned previously sent to the NPU.
- The E1 channel is mapped into a sub-interface (with specific VLAN).

- The packets received into the NPU with that specific VLAN number go through the VPWS logic and gets pseudowired (xconnected) with the configuration in a specific sub-interface.
- QOS configured under the sub-interface gets applied to this PW.

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 SDH to switch to another circuit during failure.

Consider a deployment scenario with the MR-APS circuits from a base transceiver station is connected to access router and must be transported to the base station controller through an aggregation router over an MPLS network through pseudowire. When the pseudowire reaches the router with MR-APS, data is depacketized on the smart SFP and the raw TDM frames are sent towards the base station controller. The controller is connected to routers via two links, one as working link from router-A and other as protect link towards the router-B.

Configuring Xconnect on Sub-Interface

To configure E1 port based on the VLAN ID, create sub-interface Gigabit Ethernet port.

Note The **propagate-tdm-alarm** command enables the forwarding of port level alarms to Gigabit Ethernet port in which Smart SFP resides.

```
Config terminal
controller STM1 0/0/0/0
   propagate-tdm-alarm
!
interface GigabitEthernet0/0/0/18.200 l2transport
 encapsulation dot1q 200
!


interface GigabitEthernet0/0/0/7.100 l2transport
 encapsulation dot1q 100

l2vpn
 pw-class tdm_pw
  encapsulation mpls
  !
 !
 xconnect group tdm_csop
  p2p pw200
   interface GigabitEthernet0/0/0/18.200
   neighbor ipv4 2.2.2.2 pw-id 200
    pw-class tdm_pw
   !
  !
 !
 xconnect group tdm_tpop
  p2p pw100
   interface GigabitEthernet0/0/0/7.100
   neighbor ipv4 2.2.2.2 pw-id 100
    pw-class tdm_pw
   !
  !
 !
!
```

For more information on the standby pseudowire, see *Configure Pseudowire Redundancy* in chapter *Configure Point-to-Point Layer 2 Services* of the *L2VPN and Ethernet Services Configuration Guide*.

Field-Pluggable Device (FPD) Version Upgrade for Smart SFP

Note The following steps are applicable to Channelized SDH over Packet (CSoP) STM-1 SFPs and E1 Transparent PDH over Packet (TPoP) SFPs only.

Before you begin

To upgrade the FPD version on the Cisco NCS 540 Series Routers, perform the following steps:

1. To check the existing version of the FPD, run the **show hw-module fpd** command.

   Sample output for checking the current FPD version:

```
RP/0/RP0/CPU0:router# show hw-module fpd

Wed Dec 14 07:08:08.424 UTC

Auto-upgrade:Disabled
                                                                         FPD Versions
                                                                        ==============
Location   Card type             HWver FPD device       ATR Status    Running   Programd

---------------------------------------------------------------------------------------
0/RP0      N540-ACC-SYS           0.5   MB-MIFPGA            CURRENT     0.05       0.05

0/RP0      N540-ACC-SYS           1.0   SSFP_E1F_12          NEED UPGD   7.01       7.01

0/RP0      N540-ACC-SYS           1.0   SSFP_E1F_4           CURRENT    13.01      13.01

0/RP0      N540-ACC-SYS           1.0   SSFP_STM1_TSOP_1     CURRENT    13.00      13.00

0/RP0      N540-ACC-SYS           0.5   Bootloader           NEED UPGD   1.14       1.14

0/RP0      N540-ACC-SYS           0.5   CPU-IOFPGA           NEED UPGD   0.07       0.07

0/RP0      N540-ACC-SYS           0.5   MB-IOFPGA            NEED UPGD   0.23       0.23

0/RP0      N540-ACC-SYS           0.5   SATA-M500IT-MU-B     CURRENT     4.00       4.00
```

2. To upgrade the hardware, run the **upgrade hw-module location 0/RP0 fpd <> force** command.

   To check the status of upgrade, run the **show hw-module fpd** command until the upgrade progress reaches 100 percent. The following are sample outputs for checking the status of the upgrade:

```
RP/0/RP0/CPU0:router# show hw-module fpd

Wed Dec 14 07:08:08.424 UTC

Auto-upgrade:Disabled
                                                                         FPD Versions
                                                                        ==============
Location   Card type            HWver FPD device       ATR Status    Running   Programd

---------------------------------------------------------------------------------------
0/RP0      N540-ACC-SYS          0.5   MB-MIFPGA            CURRENT     0.05      0.05

0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_12          30% UPGD   13.01
0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_4           CURRENT    13.01     13.01

0/RP0      N540-ACC-SYS          1.0   SSFP_STM1_TSOP_1     CURRENT    13.00     13.00

0/RP0      N540-ACC-SYS          0.5   Bootloader           NEED UPGD   1.14      1.14

0/RP0      N540-ACC-SYS          0.5   CPU-IOFPGA           NEED UPGD   0.07      0.07

0/RP0      N540-ACC-SYS          0.5   MB-IOFPGA            NEED UPGD   0.23      0.23

0/RP0      N540-ACC-SYS          0.5   SATA-M500IT-MU-B     CURRENT     4.00      4.00
RP/0/RP0/CPU0:router# show hw-module fpd

Wed Dec 14 07:08:08.424 UTC

Auto-upgrade:Disabled
                                                                       FPD Versions
                                                                      ==============
Location   Card type            HWver FPD device       ATR Status    Running   Programd

---------------------------------------------------------------------------------------
0/RP0      N540-ACC-SYS          0.5   MB-MIFPGA            CURRENT     0.05      0.05

0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_12          75% UPGD   13.01
0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_4           CURRENT    13.01     13.01

0/RP0      N540-ACC-SYS          1.0   SSFP_STM1_TSOP_1     CURRENT    13.00     13.00

0/RP0      N540-ACC-SYS          0.5   Bootloader           NEED UPGD   1.14      1.14

0/RP0      N540-ACC-SYS          0.5   CPU-IOFPGA           NEED UPGD   0.07      0.07

0/RP0      N540-ACC-SYS          0.5   MB-IOFPGA            NEED UPGD   0.23      0.23

0/RP0      N540-ACC-SYS          0.5   SATA-M500IT-MU-B     CURRENT     4.00      4.00
```

Procedure

Step 1 After the Smart SFP FPD upgrade completes 100 percent or after receiving the upgrade success message, wait for 15 seconds.

Step 2 Perform an online insertion and removal (OIR) of the Smart SFP:

a) Remove the Smart SFP and wait for two minutes for the clean-up to complete.

b) Insert the Smart SFP on the same port.

This step recreates the controller with all its configurations.

Step 3 To verify the Smart SFP version, run the **show hw-module fpd** command.

Sample command output for checking the FPD version of the Smart SFP:

```
RP/0/RP0/CPU0:router# show hw-module fpd

Wed Dec 14 07:08:08.424 UTC

Auto-upgrade:Disabled
                                                                         FPD Versions
                                                                        ==============
Location   Card type            HWver FPD device       ATR Status    Running   Programd
-----------------------------------------------------------------------------------------
0/RP0      N540-ACC-SYS         0.5   MB-MIFPGA            CURRENT     0.05      0.05
0/RP0      N540-ACC-SYS         1.0   SSFP_E1F_12          CURRENT    13.01     13.01
0/RP0      N540-ACC-SYS         1.0   SSFP_E1F_4           CURRENT    13.01     13.01
0/RP0      N540-ACC-SYS         1.0   SSFP_STM1_TSOP_1     CURRENT    13.00     13.00
0/RP0      N540-ACC-SYS         0.5   Bootloader           NEED UPGD   1.14      1.14
0/RP0      N540-ACC-SYS         0.5   CPU-IOFPGA           NEED UPGD   0.07      0.07
0/RP0      N540-ACC-SYS         0.5   MB-IOFPGA            NEED UPGD   0.23      0.23
0/RP0      N540-ACC-SYS         0.5   SATA-M500IT-MU-B     CURRENT     4.00      4.00
```

Cisco Smart SFP Destination MAC address

A Destination MAC address is a unique hardware address for Cisco Smart SFPs that:

- Allows seamless communication between Cisco Smart SFPs and third-party devices requiring MAC address validation
- Ensures interoperability by enabling users to configure a specific destination MAC address in the SFP, and
- Resolves validation issues caused by the default destination MAC address of 0, ensuring data packets are accepted by the destination device.

Table 3: Feature History Table

Feature Name	**Release Information**	**Feature Description**
Cisco Smart SFP Destination MAC address	Release 25.3.1	The feature is now supported on these platforms: • N540X-16Z4G8Q2C-A • N540X-16Z8Q2C-D

Feature Name	Release Information	Feature Description
Cisco Smart SFP Destination MAC address	Release 25.2.1	We now allow seamless interoperability between Cisco Smart SFPs and third-party devices that require MAC address validation. This capability is achieved by allowing the configuration of a destination MAC address directly on Cisco Smart SFPs. You can configure a specific destination MAC address on Transparent PDH over Packet (TPoP) and Channelized SDH over Packet (CSoP) Smart SFPs enabling Cisco Smart SFPs to ensure that data packets are successfully accepted by the destination device. By default, the destination MAC address on the Cisco smart SFPs is zero. The feature is supported only on: • N540-24Z8Q2C-M • NCS540-ACC-SYS

How destination MAC address helps packet transmission using Cisco Smart SFP

In today's diverse networking environments, achieving seamless interoperability in diverse networking environments is essential. When Cisco Smart SFPs interact with third-party SFPs, packet drops may occur due to MAC address validation conflicts.

By default, Cisco Smart SFPs employ a destination MAC address of 00:00:00:00:00:00 that third-party SFPs reject during validation. To ensure interoperability, configure the MAC address of the third-party SFP as the destination MAC address on the Cisco Smart SFP.

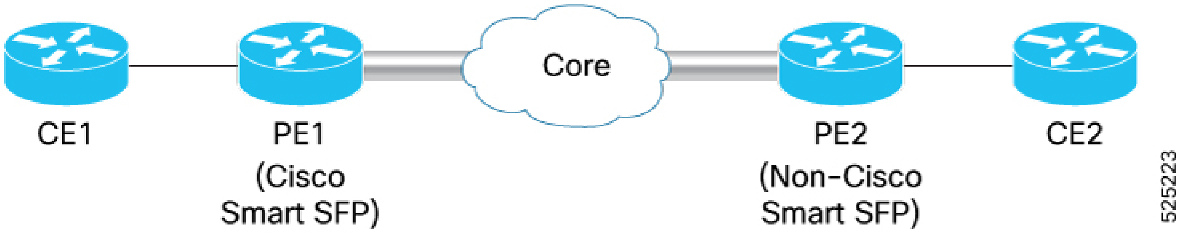
Summary

The key components involved in the packet transmission using Cisco Smart SFP with destination MAC address process are:

- **Customer Edge (CE) Routers**: These routers connect customer networks to provider networks.
- **Provider Edge (PE) Routers**: These routers manage traffic between the core network and customer networks.
- **Cisco Smart SFP**: Installed in PE1, such as Transparent PDH over Packet (tpop) and Channelized SDH over Packet (csop) Smart SFPs.
- **Non-Cisco Smart SFP**: Installed in PE2, the Non-Cisco Smart SFP validates the MAC address of incoming packets.
- **Core**: Intermediate routers in the provider network that forward data between PE routers.

Workflow

Figure 1: Packet transmission using Cisco Smart SFP with destination MAC address



The stages explain how packet transmission occurs using a destination MAC address in a Cisco Smart SFP.

1. **Destination MAC configuration**: Configure the MAC address of the peer SFP as the destination MAC address on the Cisco Smart SFP located on PE1. This ensures that all outgoing packets from PE1 carry a valid destination MAC address, meeting the requirements of the non-Cisco Smart SFP on PE2 and enabling proper packet delivery.

2. **Destination MAC verification**: The Cisco Smart SFP on PE1 uses the newly configured destination MAC address to validate the destination MAC address of incoming packets. If the destination MAC address is invalid, the Cisco Smart SFP discards these packets and records them as missing. This step ensures compliance with the MEF8 Standard 6.6.1 R.57, enhancing the reliability of packet transmission.

3. **Transmission and validation**: With the valid destination MAC address configured on PE1, the non-Cisco Smart SFP on PE2 successfully receives and processes the incoming packets. The non-Cisco Smart SFP validates the destination MAC address on the packets, confirming their correctness and enabling seamless data transmission between the two devices.

Guidelines for Cisco Smart SFP Destination MAC address

- The Cisco Smart SFPs destination MAC address feature is supported in:
  - TPOP (SFP-E1F-SATOP-I)
  - CSOP (SFP-CH-OC3STM1-I)

- The Cisco Smart SFPs destination MAC address feature is supported on:
  - N540-24Z8Q2C-M

    NCS540-ACC-SYS

    N540X-16Z4G8Q2C-A

    N540X-16Z8Q2C-D

- Configure the destination MAC address at the E1 controller level to ensure proper packet validation.

- Packets with a destination MAC address different from the configured address are dropped and counted as missing/underrun packets if incoming MAC address verification is enabled.

- When configuring the destination MAC address, always use the MAC address of the far-end device.

- **CSOP Smart SFP**

- Configuring the destination MAC address for one channel of the STM1 SFP automatically enables verification of incoming packet MAC addresses on all 63 channels
- To disable incoming packet MAC address verification, unconfigure the destination MAC address for each channel individually.
- When the destination MAC address is configured, the CSOP SFP can interoperate with only one device across all 63 channels.

Limitations for Cisco Smart SFP Destination MAC address

Incompatibility with MR-APS

The Cisco Smart SFP Destination MAC address feature is incompatible with Multi-Router Automatic Protection System (MR-APS). Since the MAC address must be reconfigured upon switchover (a process not handled automatically), avoid using this feature with MR-APS.

Configure the destination MAC Addresses on Cisco Smart SFPs

Configuring the destination MAC address on Cisco Smart SFPs to achieve seamless interoperability with peer non-Cisco SFPs that require MAC address validation.

Procedure

Step 1 Configure the MAC address of the peer Non-Cisco Smart SFP as the destination MAC address on the Cisco Smart SFP.

Example:

```
Router# config
Router(config)# controller e1 0/0/0/3
Router(config)# dmac-address 1111.2222.3333
```

This configuration enables the Cisco Smart SFP to receive packets from the Non-Cisco Smart SFP with the MAC address 1111.2222.3333.

Step 2 Use the show running configuration command to verify the controller configuration on E1 for a TPoP smart SFP.

Example:

```
Router# show run controller e1 0/0/0/3
controller E1 0/0/0/3
dmac-address 1111.2222.3333
vlan 70 ecid 7
```