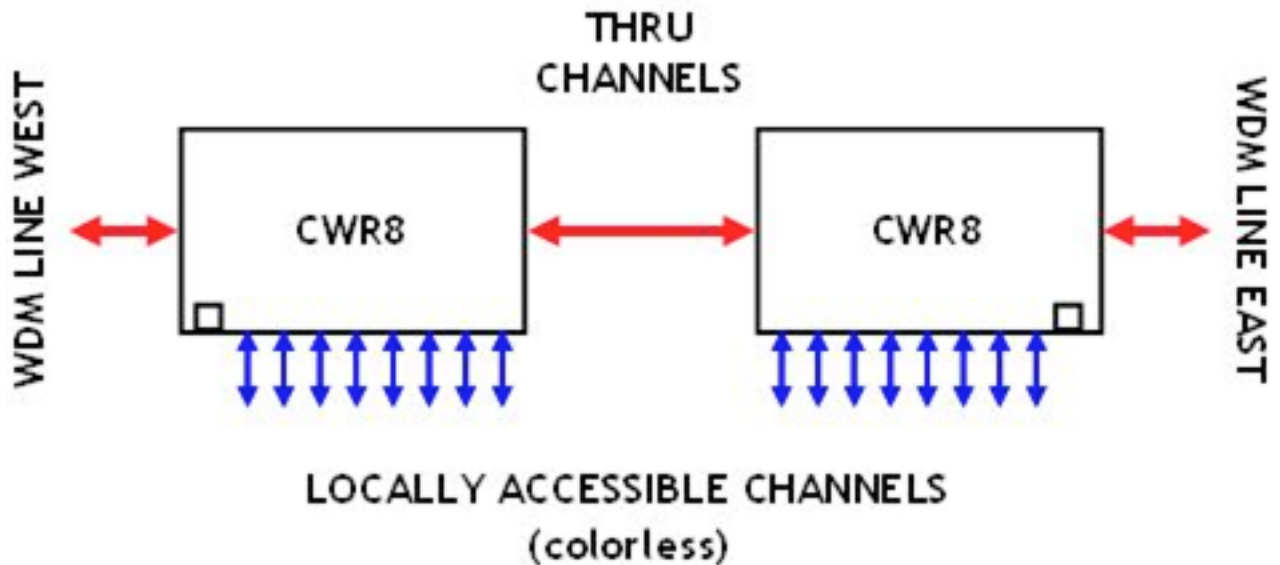


Refer to [Figure 14-5, “TOADM filter architecture \(2-degree\)”](#) (p. 14-17).

Figure 14-5 TOADM filter architecture (2-degree)



In a 2-degree TOADM, transponders can be connected to any of the eight “colorless” ports on the same CWR8 or CWR8-88 regardless of transmission wavelength—simplifying wavelength adds. During reconfiguration, tunable transponders can tune to a new wavelength without the need for any manual re-fibering. This combination of wavelength switching, colorless add/drop, and tunable transponders yields a fully remotely reconfigurable optical node, of which the ROADM was only a first step.

Additionally, the start-up cost of the TOADM is less than the ROADM because no static filters are required; colorless add-drop ports are inherently part of the Alcatel-Lucent 1830 PSS-32 CWR8/CWR8-88 wavelength router architecture.

Colorless ports are also used for interconnection of additional CWR8/CWR8-88 packs for higher degree TOADM nodes. Therefore, for a 3-degree TOADM, there is one less colorless port for transponders: seven; for 4-degree TOADM: six.

In future releases, CWR8/CWR8-88 wavelength routers will be optionally cascaded for up to a 44-colorless-channel TOADM.

Also in a future release, a CWR8/CWR8-88 cascade will be able to effect a “directionless” TOADM. In the “standard” TOADM of Alcatel-Lucent 1830 PSS-32, each CWR8/CWR8-88 is associated with a particular WDM line (degree), and a transponder connected to that CWR8/CWR8-88 is also associated with that line. In a directionless TOADM, a transponder can be switched to different optical lines without any re-fibering.

Note: The CWR8B is interchangeable with the CWR8 and can be used in the applications described here.

CWDM

CWDM Overview

Compared to DWDM networks, CWDM networks have lower capacity and shorter optical reach; however they are also lower in cost for certain applications where they are suitable. Support for CWDM on Alcatel-Lucent 1830 PSS-32, Alcatel-Lucent 1830 PSS-16, and Alcatel-Lucent 1830 PSS-4 shelves is another instance of the product's flexibility to cost-optimize for any application, in this case usually for Metro Access.

Alcatel-Lucent 1830 PSS-32, Alcatel-Lucent 1830 PSS-16, and Alcatel-Lucent 1830 PSS-4 shelves support up to eight CWDM wavelength channels from the standardized optical grid specified by the ITU-T G.694.2 recommendation. Channel spacing is 20 nm. The eight channels are 1471, 1491, 1511, 1531, 1551, 1571, 1591, and 1611 nm.

When a Alcatel-Lucent 1830 PSS-32, Alcatel-Lucent 1830 PSS-16 or Alcatel-Lucent 1830 PSS-4 shelf is configured to support CWDM, it shares all the same hardware as DWDM and is supported out of the same shelf. That is, a node can be on a DWDM ring with a CWDM spur. The major hardware differences are that a CWDM line uses CWDM filters, is not amplified, and uses an embedded GCC channel instead of an OSC for supervisory communications.

CWDM filters

1830 PSS Release 8.2 includes three filter types.

- SFC8: 8 add/drop channels; no pass-through channels. 1 variant.
- SFC4x: 4 add/drop channels; 4 pass-through channels. 2 variants: x=A, B
- SFC2x: 2 add/drop channels; 6 pass-through channels. 4 variants: x=A, B, C, D.

Refer to [Table 14-3, "CWDM filter scheme" \(p. 14-19\)](#)

Table 14-3 CWDM filter scheme

Wavelength (nm)	SFC2	SFC4	SFC8
1471	SFC2A	SFC4A	SFC8
1491			
1511	SFC2B		
1531			
1551	SFC2C	SFC4B	
1571			
1591	SFC2D		
1611			

These filters do not support an OSC channel. Management information is communicated node-to-node using the embedded GCC channel.

CWDM optical interface

In 1830 PSS Release 8.2, a CWDM spur off of a DWDM ring can be realized by plugging a CWDM SFP or XFP into a client port of an 1830 PSS-32/16 optical transponder, which can connect to CWDM sub-tending equipment on the spur's far end.

Two cases can be considered:

- A CWDM XFP can be used on the client side of the 11STAR1 transponder. Two reaches are available: 40 and 80 km. In this case, if the sub-tending device is an Alcatel-Lucent 1830 PSS-1 GBEH or 1830 PSS-1 MD4H edge device, then the Alcatel-Lucent 1830 PSS management domain can be extended via the embedded GCC channel.
- A CWDM SFP can be used on the client side of the 11STGE12 and 11STMM10 transponders. 80 km reach is available.

Transponders with tunable line-side lasers support DWDM wavelengths. Transponders with PTM line-side interfaces can support DWDM or CWDM XFPs.

DWDM topologies

DWDM topology overview

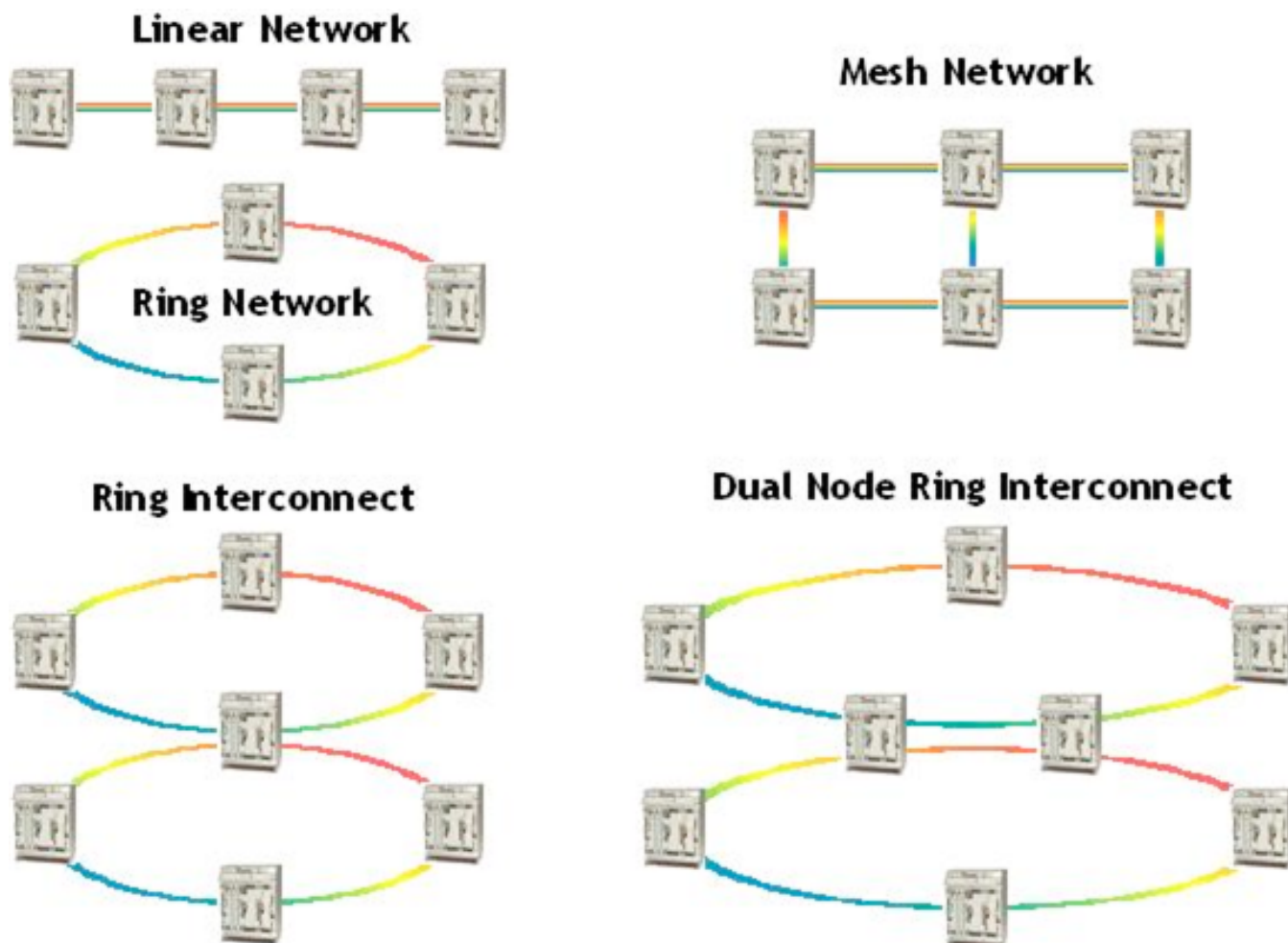
The 1830 PSS-32 and PSS-16 support an almost unlimited number of DWDM network configurations and combined network configurations. Some of these configurations are listed below. For more detailed information, refer to [Chapter 17, “WDM topologies and configurations”](#). The Alcatel-Lucent 1830 PSS-16 is targeted primarily for FOADM applications.

- Simple point-to-point and linear topology with optical add-drop
- Ring topology with optical add-drop
- Transparent ring interconnection using multi-degree nodes with local add-drop
- Additional mesh networking, e.g., in dual-node ring interconnection.

In these networks, each of the nodes can be FOADM, ROADM, or TOADM, although the multi-degree nodes that perform ring interconnection would normally be ROADM or TOADM.

Examples of these topologies are shown in [Figure 14-6, “Example: DWDM networks for FOADM, ROADM, and TOADM”](#) (p. 14-22).

Figure 14-6 Example: DWDM networks for FOADM, ROADM, and TOADM



From such networks, spurs and dual-homed nodes can be added, as shown in [Figure 14-7, “Spurs and dual-homed nodes”](#) (p. 14-23).

In these cases there is no need for reconfigurability at the access node, so typically FOADMs are deployed.

Figure 14-7 Spurs and dual-homed nodes



Transmission features

Overview

Purpose

This section provides information related to WDM transmission features of Alcatel-Lucent 1830 PSS.

Contents

Bidirectional CWDM single-fiber transmission	14-25
Optical amplification and dispersion compensation	14-26
Automatic power reduction (APR)	14-32
Optical transponders	14-56
WDM Protection	14-58

Bidirectional CWDM single-fiber transmission

Overview

The 1830 PSS-32 and PSS-16 support nodes with CWDM bi-directional transmission over a single fiber.

Note: DWDM single fiber transmission is not supported.

Bidirectional transmission over a single fiber is supported with any of the following filters and OTs:

- SFC2(A, B, C, or D)
- SFC4(A or B)
- SFC8
- 4DPA4
- 4DPA2
- 11STAR1
- 11STMM10

For details about optical connections to provision single-fiber operation see [“Single-fiber bi-directional nodes”](#) (p. 17-191).

Optical amplification and dispersion compensation

Amplifier overview

Optical amplifiers provide several important functions that comprise optical transport section of a DWDM optical line, including:

- Optical amplification
- Optical supervisory channel (OSC) generation/termination
- Dispersion compensation access points
- Optical line and individual optical channel monitoring points
- Optical monitoring access point (OSA access point for non-intrusive monitoring with external equipment)
- Electrical access point for remote passive module inventory monitoring (DCM and/or SFD44/SFD44B modules)

Optical amplification function is performed through multistage EDFA amplifiers, most with mid-stage DCM access. These amplifiers are implemented as integrated variable gain optical amplifier modules (VGOAM) that include fast feedback for transient control.

Unidirectional and bidirectional amplifiers

Amplifiers that are bidirectional carry optical signals in both directions, however only one direction has amplification. The other direction is a through connection without amplification. As a result bidirectional amplifiers in an ILA are used in a schematic “back-to-back” arrangement where the amplified signal from one amplifier passes through the non-amplified path of its partner. The connections for this arrangement are shown in [Figure 17-154, “ILA with bidirectional LDs and optional RA2Ps ” \(p. 17-187\).](#)

Amplifiers that are unidirectional have a single amplified path through them. As a result unidirectional amplifiers in an ILA are used in a schematic “side-by-side” arrangement where only a single signal, in one direction, passes through each amplifier and is amplified. The connections for this arrangement are shown in [Figure 17-155, “ILA-2: ILA with unidirectional LDs and optional RA2Ps” \(p. 17-187\).](#)

The optical amplifiers supported on Alcatel-Lucent 1830 PSS WDM shelves are shown in the following table along with the release in which they were introduced and the shelves and OADM types in which they are supported.

Table 14-4 Optical Amplifiers

Type	Description	PSS-8	PSS-16	PSS-16II	PSS-32	OADM's
AAR-8A	AAR-8AAmp Array 8-amps	-	-	R8.1	R7.0.2	CDC-F ROADM

Table 14-4 Optical Amplifiers (continued)

Type	Description	PSS-8	PSS-16	PSS-16II	PSS-32	OADM's
ALPHG	Low Power High Gain DWDM Amplifier with mid-stage access, for application in 88 channel short spans (Bidirectional)	-	R2.5	-	R1.0	TOADM, ROADM, DFOADM
AHPHG	High Power High Gain DWDM Amplifier with mid-stage access, for application in 88 channel long spans (Bidirectional)	R8.0.2	R2.5	-	R1.0	TOADM, ROADM, DFOADM
AHPLG	High Power Low Gain DWDM Amplifier with mid-stage access. An 88 channel Bidirectional Egress Amp, for application in an ILA and Ingress for spans < 20 dB, or ILA and Ingress with an RA2P Pre-Amp.	R8.1	R2.5	-	R2.0	TOADM, ROADM, DFOADM
A2325A	Amplifier, 23 dB power, variable gain, C-band, with mid-stage access, for application in an 88 channel ILA and Ingress for spans > 20 dB (Bidirectional)	R8.0.2	R2.5	-	R2.5	TOADM, ROADM, DFOADM
AM2125A	High power (+21 dBm), 25 dB gain optical amplifier with mid-stage access, for application in DCU free applications and FBG DCU's, or ILA and Ingress for spans > 20 dB (Unidirectional)	R8.0.2	R3.5	-	R3.5	TOADM, ROADM
AM2125B	High power (+21 dBm), 25 dB gain optical amplifier without mid-stage access (Unidirectional)	R8.0.2	R3.5.2	-	R3.5.2	TOADM, ROADM

Table 14-4 Optical Amplifiers (continued)

Type	Description	PSS-8	PSS-16	PSS-16II	PSS-32	OADM's
AM2318A	Low variable gain amplifier with no DCM access (Unidirectional)	R8.0.2	R3.6	-	R3.6	TOADM, ROADM
MESH4	The four output MESH pack (MESH4) is a uni-directional LD type pack that monitors and amplifies an input signal then splits it into four outputs. It is used to split a WR pack MESHOUT into four signals (Unidirectional).	-	R5.0	-	R3.6	ROADM
RA2P	Long Haul - 2 pump Raman module, no mid-stage access, for application as an External booster for long spans, or Raman Preamp for long reach (Unidirectional)	R8.0.2	R3.5	-	R3.5	TOADM, ROADM, DFOADM
A2P2125	Hybrid LD, consisting of a high-power VGOAM-MMG module, similar to AM2125B, and a Raman module, similar to RA2P (Unidirectional)	-	R5.5	-	R5.5	ROADM
AM2625A	Variable high gain Amplifier with mid-stage access	-	R7.0	-	R7.0	ROADM, DFOADM
AM2032A	Variable gain Amplifier with mid-stage access	-	R7.0	-	R7.0	ROADM, DFOADM
ASWG	Switched Gain EDFA	-	R7.0	R8.1	R7.0	ROADM CDC-F, DGE CDC-F

Table 14-4 Optical Amplifiers (continued)

Type	Description	PSS-8	PSS-16	PSS-16II	PSS-32	OADM's
A4PSWG	Switched Gain Hybrid Amplifier for ULH	-	R7.0	R8.1	R7.0	ROADM CDC-F, DGE CDC-F

The OAs have the following features:

- Support for all Alcatel-Lucent 1830 PSS universal shelf configurations in the C-band
- Variable gain amps: two stages of EDFA amplifiers with mid-stage access for DCMs in between (except AM2325B and AM2017B)
- Variable gain amps: no LBOs are required except at mid-stage when there is no DCM (except AM2625A)
- Integrated, provisionable tilt control (necessary for FOADM nodes; in TOADM nodes the CWR8/CWR8-88 performs optical equalization)
- Transient support

Optical supervisory channel (OSC)

Inter-node management and control information is communicated over the OSC. The OSC wavelength is at 1510 nm and is terminated on the amplifiers, or non-amplified OSC card, through SFP PTM. Three different OSC SFPs support three different ranges of span losses.

OSC provides high-speed data communication channel between adjacent OTS lines as well as maintenance, monitoring, and customer clear channel communication function. OSC is implemented as OC-3 compliant digital structure with ~149 Mb/s payload capacity for data communication and clear-channel transport. Physical layer of OSC channel is implemented as 1510 nm OC-3 SFP. An OSCT card is used to for applications where the optical span is so short, that an optical amplifier is not required.

Note: Raman amplification in the span can extend OSC reach to about 43 dB, depending on fiber plant, point losses, and overall available Raman gain in that span. The RA2P and AM2625A, when used together, can extend this reach up to about 50 dB. However, there may be minimum channel loading requirements on the RA2P. (See the Alcatel-Lucent 1830 Photonic Service Switch (PSS) Raman Amplifier and Erbium Doped Fiber Amplifier (EDFA) User Guide.)

Refer to [Table 14-5, “OSC SFP span loss support”](#) (p. 14-30).

Table 14-5 OSC SFP span loss support

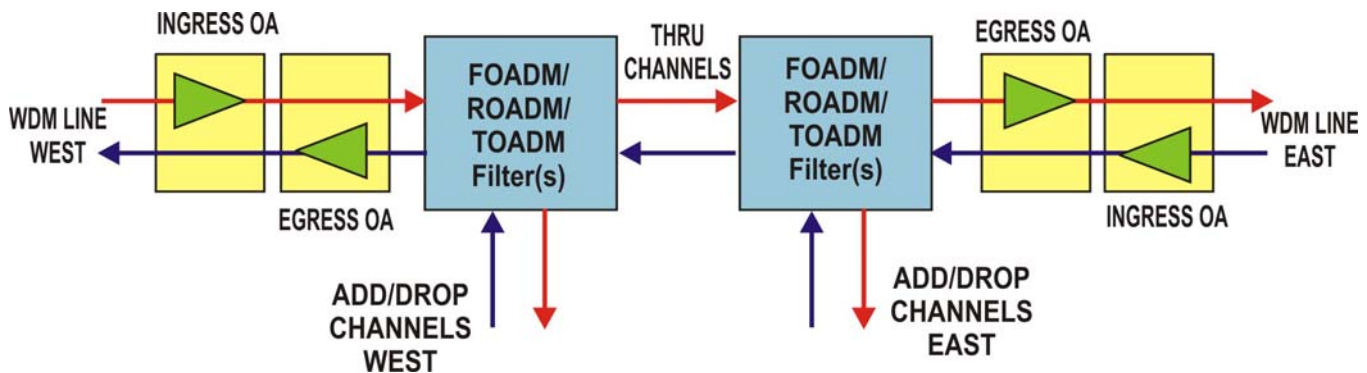
OSC SFP	Span loss range (dB) (measured at 1545 nm)
Short reach	4 to 16
Long reach	11 to 26
Ultra-long reach	14 to 33
Extended ultra-long reach	15 to 40

Amplifier node configuration

The Alcatel-Lucent 1830 PSS WDM shelves optionally use an optical amplifier at the ingress to the node, and optionally at the egress. The ingress amplifier also provides OSC termination in both directions.

Refer to [Figure 14-8, “Node optical architecture”](#) (p. 14-30)

Figure 14-8 Node optical architecture



Any of the ALPHG, AHPHG, AHPLG, and A2325A can be used in either position, allowing for a wide range of flexibility. The *Alcatel-Lucent 1830 Engineering and Planning Tool* will determine the optimal combination of amplifiers.

Note: An A2325A, AM2125A, AM2125B, or AM2318A amplifier in the ingress position is only supported in WR8-88A/WR8-88AF ROADM, WR2-88 ROADM, TOADM, and ILA nodes. It is not supported in FOADM configurations.

Note: In TOADM applications where the ingress amplifier is AM2125A or AM2125B, the egress amplifier must be the same type amplifier as the ingress, or can be an AM2318A. In TOADM applications where the ingress amplifier is AM2318A, the egress amplifier must be an AM2125A, AM2125B, or AM2318A.

For a complete list of supported amplifier combinations in FOADM DFOADM, and ILA configurations, see [“Supported LD combinations for OADM and ILA configurations” \(p. 22-128\)](#).

For spans with more than 40 dB loss, an external Raman amplifier can be used with an EDFA booster.

The Optical Supervisory Card Total Power (OSCT) card is also available to provide OSC termination, but without any amplifiers. It is cost-optimized for very short spans not requiring amplification. (See [“Optical supervisory card total power \(OSCT\)” \(p. 18-246\)](#).)

Chromatic dispersion compensation

For long all-optical routes, the Alcatel-Lucent 1830 PSS-32/Alcatel-Lucent 1830 PSS-16 uses dispersion compensating modules (DCMs) to compensate for chromatic dispersion on the line fiber. The granularity of the DCM lengths ensures that proper compensation can be achieved flexibly. Depending upon fiber type, DCMs are available for compensating at increments as shown in the following table:

Fiber	Granularity (km)	Span (km)
SSMF	10	10-140
SSMF (negative)	10	10-30
TWRS	20	20-120
ELEAF	20	20-120

DCMs are installed at the mid-stage of optical amplifiers and compensate for the line associated with the amplifier.

In-line amplifier (ILA) node

In some physically larger networks, the distance between two add/drop nodes may exceed the system's single span optical reach. In such a case, an ILA can be installed at a mid-point, thereby creating two shorter spans and boosting the signal strength before it gets too close to the noise floor.

Like an Alcatel-Lucent 1830 PSS-32/Alcatel-Lucent 1830 PSS-16 add/drop node, an ILA node is an individually managed network element, but without channel add/drop capabilities. It uses a subset of the same hardware to provide bidirectional line amplification and dispersion compensation only.

In very long distance applications, multiple ILAs can be installed at multiple points along the line.

Automatic power reduction (APR)

APR overview

APR is a mechanism that responds to a span cut, a fiber disconnection between nodes, or any combination of events that provide a similar indication. APR will also occur in response to certain circuit pack failures or to fiber cuts within a node when needed to meet safety requirements. APR automatically reduces power to prevent levels at an open fiber that could result in injury to personnel, or damage to equipment.

Proper operation of APR requires that the shelf with packs that are involved in the APR process be equipped with a working Equipment Controller. The EC is involved in communications between the ingress LD that monitors for line cuts, and the pack or packs that must be shut down in response to a line cut. The EC is also involved in communications between the monitoring pack and the pack that undergoes APR for fiber cuts within a node. If the packs involved in an APR process occupy more than one shelf, then a working EC is required in each shelf, and a communication path through working ECs must be available between the shelves.

Note: For the new IROADM cards, the monitoring and shutdown occur on the same pack and hence IROADMs do not require ECs for APR in response to line cuts. There are no APR conditions for fiber cuts within a node when IROADMs are used.

As currently implemented, APR will shut down the egress amplifier whenever there is a span cut or fiber disconnection, irrespective of the egress amplifier's output power prior to the cut. The software does not check whether the egress amplifier is capable of exceeding class 1M power levels, or whether it is currently operating at a level that is above class 1M.

Note: When an egress amplifier is shut down due to APR, an egress adjustment or add loop adjustment is not possible, and will fail.

APR on the 1830 PSS-32/PSS-16/PSS-4 operates under the following conditions:

- APR is performed on the egress amplifier that launches into a span that has been cut or disconnected.
- APR is performed on the amplifier at an ILA site that launches into a span that has been cut or disconnected.
- A span without an egress amplifier is cut or disconnected from an add/drop or terminal node, there is no impact on the output power of the node.
- The time between the cutting of a fiber and the completion of APR for the affected set of amplifiers is less than 3 seconds.
- Power will be restored to an egress amplifier that has been shut down due to an APR condition, no earlier than 100 seconds after detection of the event that triggered APR.

OSC requirements

Alcatel-Lucent 1830 PSS APR relies on the OSC. The OSC carries a remote defect indicator in its SONET overhead to indicate if the originating nodes see a fiber cut. Detection of the RDI, in the case of a single fiber cut, will indicate the need to shut down. When the RDI clears, it indicates that the egress amplifier can be turned on again.

When RA3P is used, the OSC should always be provisioned for OC-3 operation.

At an OADM or ILA site, if there is a high-power egress LD, the OSC for the ingress LD should be set to OC-3. If the OSC for the ingress LD is in any of the following states, it will be treated as equivalent to OSC LOS for the purposes of triggering `APR-Line` on the egress LD:

1. OSC set to port state down
2. OSC not provisioned or de-provisioned
3. OSC SFP removed
4. OSC SFP failed
5. OSC provisioned to 100BASE-FX

This requirement applies to the following LD's:

- A2325A
- AM2125A
- AM2125B
- AM2318A
- AM2625A
- A2P2125 – (applies to the Line Out port, when A2P2125 is used at an ILA)
- ASWG
- A4PSWG

An `APR-Active-Line` condition cannot be cleared on any of the above LD cards when the OSC is in one of the listed states. The OSC must first be provisioned to OC-3.

The same behavior occurs for an RA2P if the OSC on the ingress LD that follows the RA2P is set to any of the listed states, and to the Raman amplifier sections of A2P2125 and A4PSWG if the OSC on those packs are set to any of the listed states.

Note: AM2625A contains an amplifier for the OSC as well as an amplifier for the DWDM channels. As a result, if an AM2625A loses power, is removed, or undergoes a cold/hard reboot, the transmitted OSC and the transmitted DWDM channels will both shut down. This will lead to an `APR-Line` condition at the node that is downstream from the AM2625A.

LD protective cover switches

Starting in Release 3.5.0, packs that contain amplifiers that can emit power levels exceeding Class 1M have protective covers. When the cover is removed, a switch will detect the removal.

Output port (AM2125A, AM2125B, AM2318A, ASWG, AM2625A)

When a cover is removed from the output port of an LD equipped with a protective cover switch, the optical amplifier in the LD will shut down. The shut down will occur within 150 ms of the time that the cover is removed. An `APR-Active Port Switch` condition will be raised against the output port of the LD. This behavior currently applies to the AM2125A, AM2125B, AM2318A, ASWG and AM2625A LINE OUT ports.

Input port (RA2P)

When a cover is removed from the LINE IN port of Raman card equipped with a protective cover switch, the Raman pumps in the card will shut down. The shut down will occur within 150 ms of the time that the cover is removed. An `APR-Active Port Switch` condition will be raised against the LINE IN port. This behavior currently applies to the RA2P.

Input/output port (A2P2125, A4PSWG)

A2P2125 and A4PSWG have the same port cover switch behavior for both input and output ports. One switch covers both ports. Both the Raman amplifier section and the EDFA section shut down when the cover is removed, and `APR-Active Port Switch` alarm is raised.

APR examples

The following examples illustrate how 1830 PSS-32/PSS-16 APR functions to shut down and restore power in response to single and dual fiber cuts.

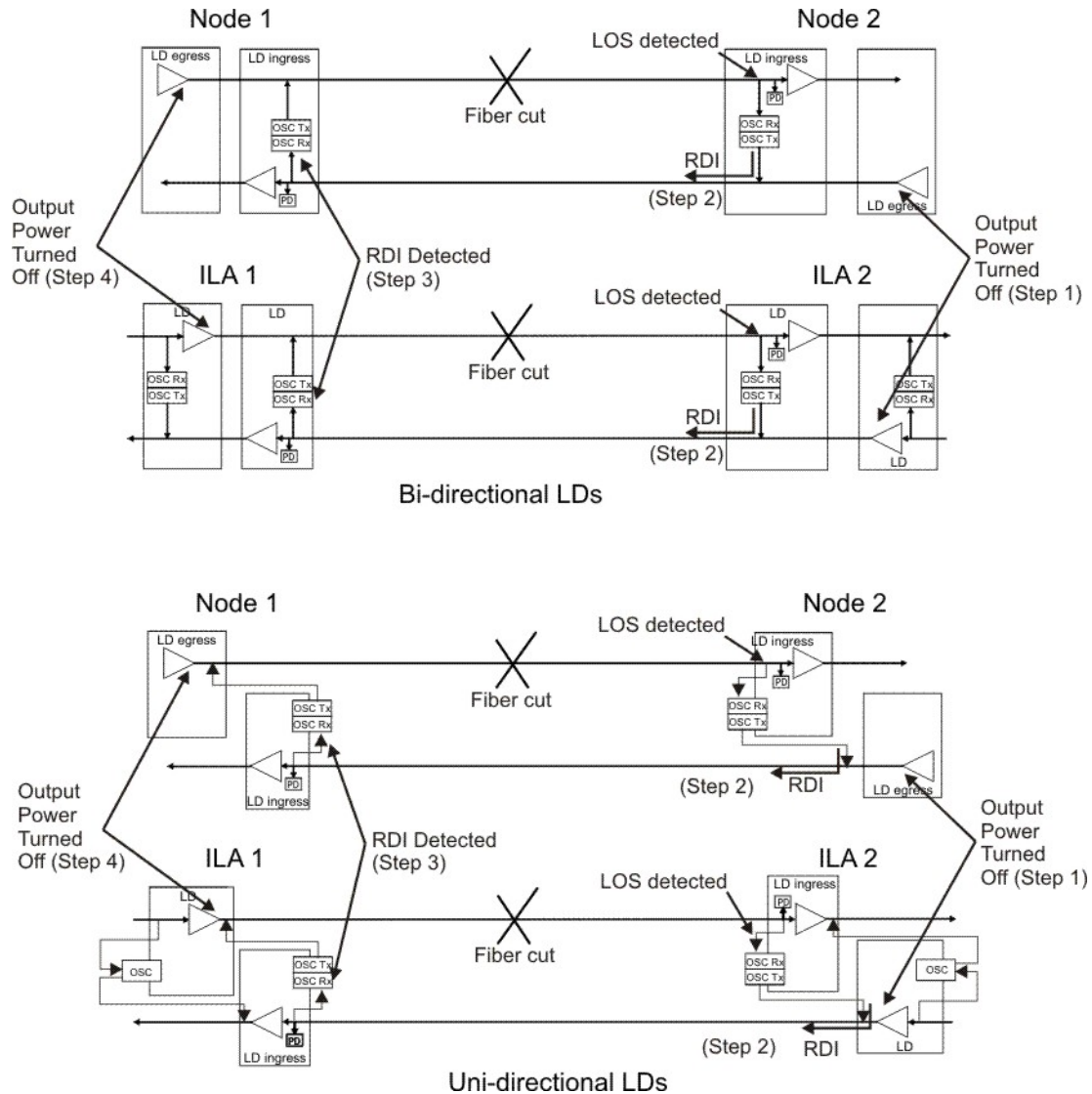
Single fiber cut shutdown

A span cut on the transmission path from Node 1/ILA 1 to Node 2/ILA 2, as shown in [Figure 14-9, “Single fiber cut” \(p. 14-35\)](#), will result in LOS for both the DWDM channels and the OSC at the detection points indicated in the illustration. In some failure cases, noise might be present on the OSC channel, but not signal, so other OSC failures are also used to trigger APR (LOF, LOL). The presence of both DWDM and OSC defects will trigger a shutdown.

This shutdown will occur as a result of the following conditions:

- DWDM LOS is detected at the input to the line driver (LD) card in Node 2/ILA 2
- An OSC failure, measured by LOS, LOL, or LOF is detected at the input to the LD card in Node 2/ILA 2
- The DWDM and OSC defects continue for 10 ms

Figure 14-9 Single fiber cut

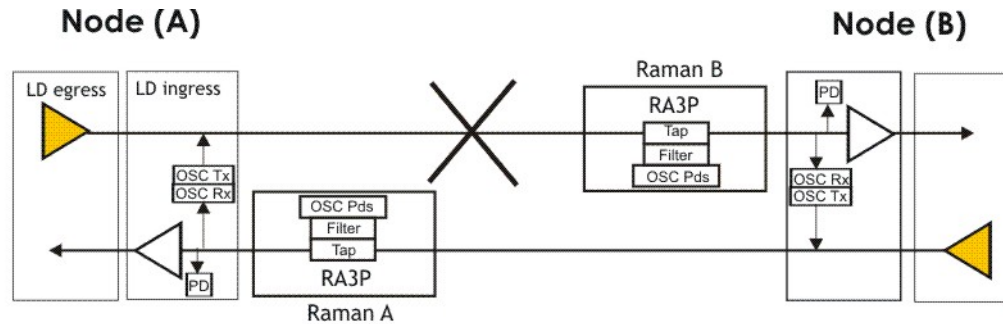


As a result of these conditions the following procedure steps will take place to implement APR:

1. The output power will be turned completely off in the Node 2/ILA 2 amplifier that amplifies DWDM channels that are transmitted back to Node 1/ILA 1, as indicated in [Figure 14-9, "Single fiber cut" \(p. 14-35\)](#).
2. The OSC transmitter in Node 2/ILA 2 will transmit a remote defect indicator (RDI) back to Node 1/ILA 1.
3. The OSC receiver in Node1/ILA 1 detects the RDI.

4. The output power is turned completely off in the amplifier in Node1/ILA 1 that amplifies the DWDM channels that are transmitted to Node 2/ILA 2.
5. Software will raise the `APR-Active-Line` condition against the output ports of the amplifiers that are shut off.

RAMAN behavior (external RA3P)



When a single direction is cut on a span containing Raman amplifiers, the Raman amplifier on the node ingress from span where there is fiber cut (Raman [B]), will see OSC loss. Its pumps will be turned off. However, Raman (A) on the side where there is no fiber cut, does not see OSC loss and does not turn the pumps off. Raman packs are completely dependent on OSC loss for APR.

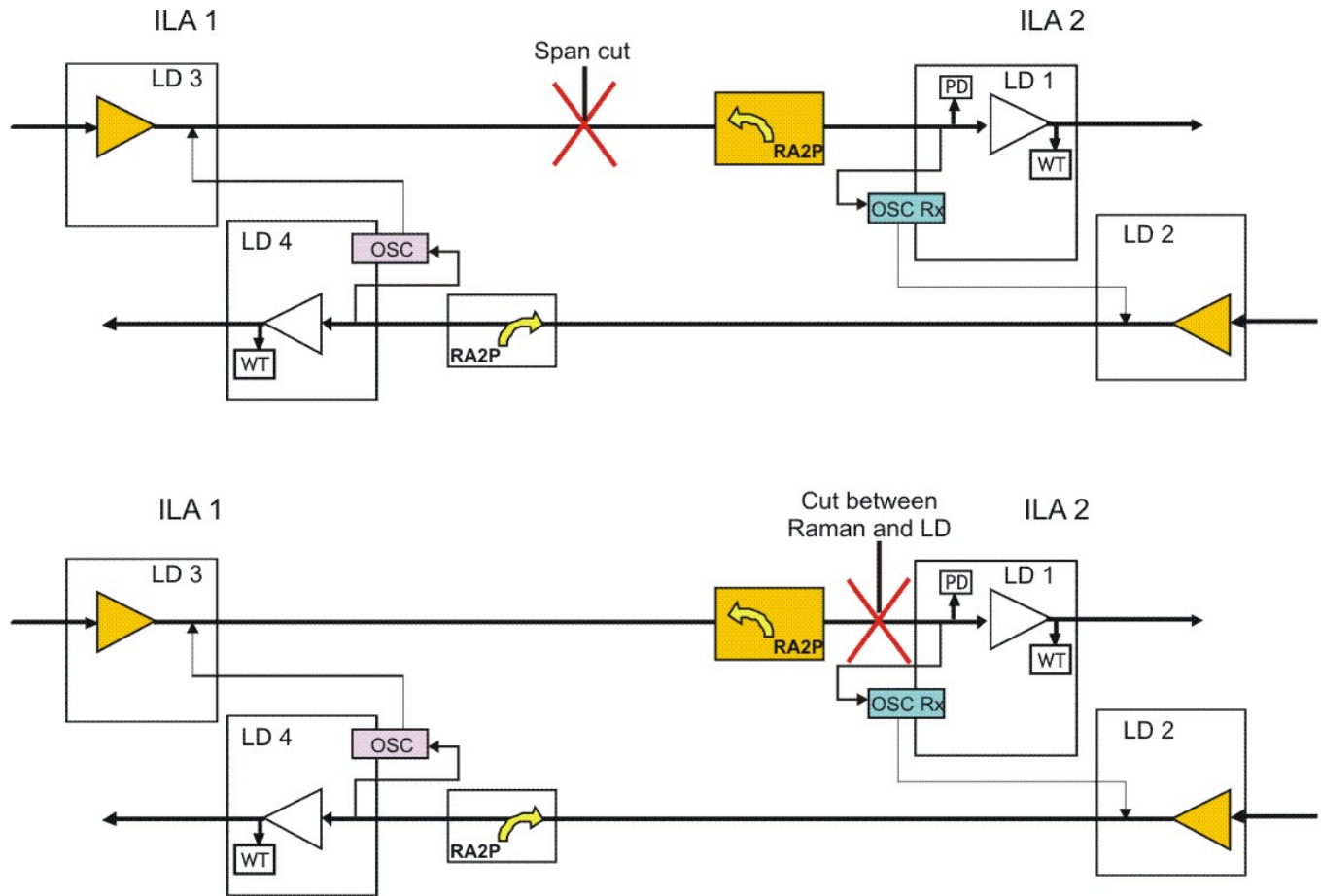
Note: IMPORTANT: The OSC must be provisioned to OC-3 for proper APR operation when an RA3P is used.

Raman behavior within NE (RA2P)

The RA2P is a Raman amplifier card that can be used with either unidirectional or bidirectional LD's. The RA2P counter-pumps the span, so it is always used at the input to a node or ILA. Unlike the RA3P, the RA2P is part of the network element.

A span that is pumped with a Raman amplifier will have a large amount of ASE noise generated within the C-band. Because the received ASE can mask the LOS condition, it is not possible to use the DWDM payload LOS to detect a fiber cut. Different triggers are used depending on the ingress LD that follows the Raman amplifier. For some LD's, APR is triggered from an OSC defect (LOS...) or any of the states that are treated as OSC defects. For other LD's, an OSC defect or equivalent state plus Loss of Tones (LOT-Out) are used to trigger APR. The OSC and, if applicable, the `LOT-OUT` detection are performed in the line-facing LD card, not in the Raman amplifier card. For more information see, ["OSC requirements"](#) (p. 14-33).

Figure 14-10 Raman RA2P single fiber cut examples



OSC LOS will occur when there is a fiber cut on a span or between the Raman amplifier and the line-facing LD, as shown in the illustration above. Therefore, the response to each event will be the same.

An OSC failure of 10 ms or longer, measured by LOS, LOL, or LOF at the input to the LD card in node or ILA2 (at the OSC SFP shown in blue in Fig. 19) will result in the following:

1. Output power will be turned off in the node or ILA 2 amplifier that amplifies DWDM channels that are transmitted back to node 1. (This is the amplifier that is colored gold in node 2 or ILA2 in the illustration above.)
2. The Raman pumps are shut down in the Raman amplifier in node/ILA 2 that counter-pumps the span that has been cut.
3. The OSC transmitter in node or ILA 2 will transmit a remote defect indicator (RDI) back to node or ILA 1.

4. When the OSC receiver (shown in pink) in node or ILA 1 detects the RDI, output power will be turned off. This is the amplifier that is colored gold in the illustration above.
5. Software will raise the `APR-Active-Line` condition against the amplifiers that are shut off. These are the gold-colored amplifiers in the LD's of nodes/ILA's 1 and 2 and the LINE IN port of the Raman amplifier in node/ILA2.

Beginning in Release 3.6.50, software will use a second trigger, loss of tones (LOT-Out), along with OSC LOS to determine when shutdown is needed. This second trigger will be used only on AM2318A, AM2125A, and AM2125B ingress LD's. For other LDs the previous Raman RA2P single fiber cut behavior, described above, still applies.

On AM2318A, AM2125A, and AM2125B ingress LD's, a single fiber cut will be detected when all of the following are present:

- An OSC failure, measured by LOS, LOL, or LOF at the input to the LD card in node or ILA2 (the OSC SFP colored blue in the illustration above)
- LOT-OUT is detected at the WT detector following the amplifier module in the same LD card in node/ILA2, or there is a failure of the WT DSP
- The OSC and the LOT-OUT defect (if applicable) remain for at least 10 ms

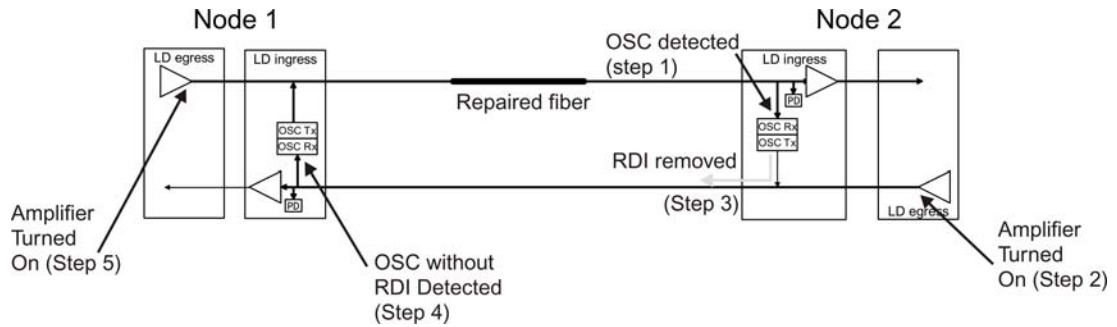
When these conditions are observed, the following will occur:

1. The output power will be turned off in the node or ILA 2 amplifier that amplifies DWDM channels transmitted back to node 1.
2. The Raman pumps are shut down in the Raman amplifier in node/ILA 2 that counter-pumps the span that has been cut.
3. The OSC transmitter in node or ILA 2 will transmit a remote defect indicator (RDI) back to node or ILA 1.
4. When the OSC receiver in node or ILA 1 detects the RDI, output power will be turned completely off in the amplifier in node or ILA 1 that amplifies the DWDM channels transmitted to node 2.
5. Software will raise an `APR-Active-Line` condition against the amplifiers that are shut off.

Restart after repair of a single fiber cut

When the cut fiber from Node 1 to Node 2 is repaired, the following procedure will take place. (Power is restored between ILAs following the same procedure.)

Figure 14-11 Single fiber restoration



1. The OSC receiver at the incoming LD in Node 2 detects the OSC from Node 1.
2. In response, the LD in Node 2 that amplifies the DWDM channels transmitted toward Node 1 is turned back on.
3. Also in response to detection of the OSC, the RDI is removed from the OSC that is transmitted from Node 2 to Node 1.
4. After the OSC without an RDI is detected at Node 1.
5. The amplifier in Node 1 that amplifies the DWDM channels transmitted toward Node 2 is turned back on.
6. The APR-Active-Line condition is cleared.

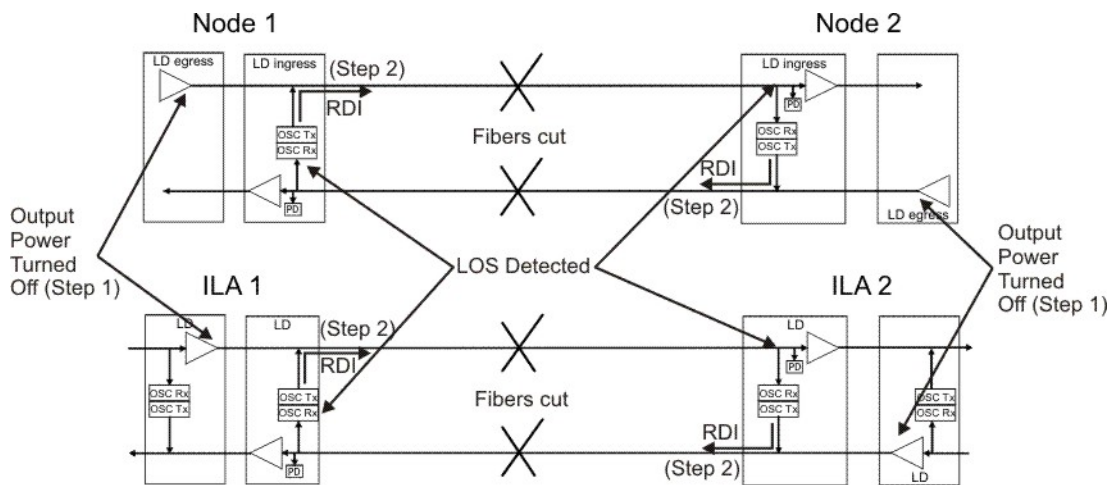
Double fiber cut shutdown

The algorithm that is followed when both fibers are cut or disconnected between two nodes/ILA's is the same as for a single fiber cut. The response is described below. A span cut on both fibers between Node 1/ILA 1 to Node 2/ILA 2, as shown in [Figure 14-12, "Double fiber cut" \(p. 14-40\)](#), will follow the same general procedure as for a single fiber cut.

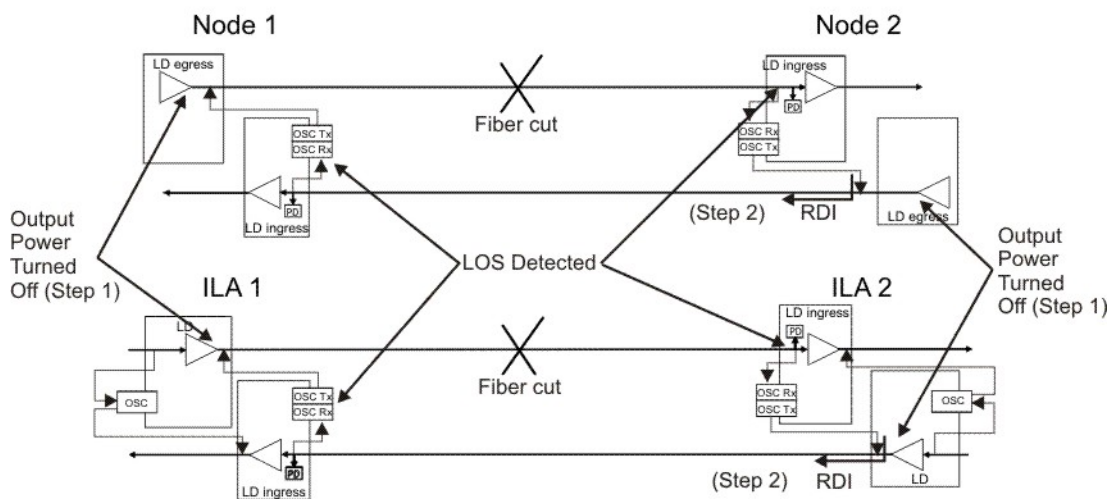
This shutdown will occur as a result of the following conditions:

- DWDM LOS is detected at the input to the LD cards in Node 1/ILA 1 and Node 2/ILA 2
- OSC failures, measured by LOS, LOL, or LOF are detected at the input to the LD cards in Node 1/ILA 1 and Node 2/ILA 2
- The DWDM and OSC defects continue for 10 ms

Figure 14-12 Double fiber cut



Bi-directional LDs

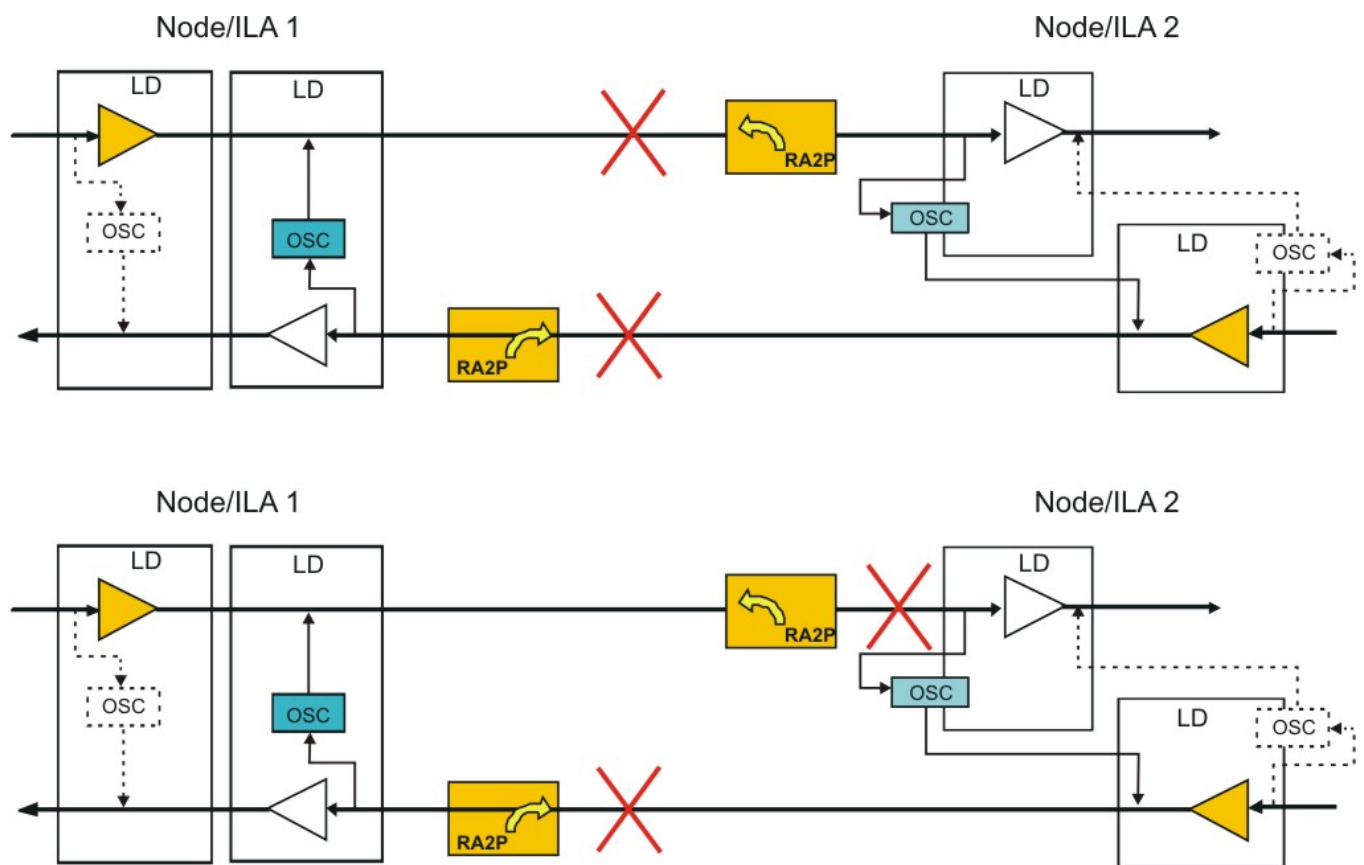


Uni-directional LDs

As a result of these conditions the following procedure steps will take place to implement APR:

1. The output power will be turned completely off in the Node 1/ILA 1 amplifier that amplifies DWDM channels transmitted to Node 2/ILA 2, and in the Node 2/ILA 2 amplifier that amplifies DWDM channels transmitted to Node 1/ILA 1.
2. The OSC transmitter in Node 1/ILA 1 will transmit a remote defect indicator (RDI) to Node 2/ILA 2 and the OSC transmitter in Node 2/ILA 2 will transmit an RDI to Node 1/ILA 1.
3. Software will raise the APR-Active-Line condition against the output ports of the amplifiers that are shut off.

RA2P LDs with double fiber cut



When an fiber cut is detected at the input to one of the line-facing LD cards, as shown above, the following events will take place:

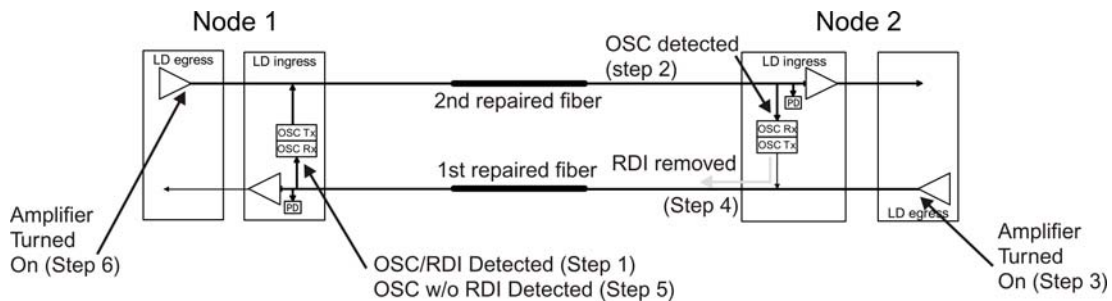
1. The output power will be turned off in the node/ILA 1 amplifier that amplifies DWDM channels transmitted to node 2, and in the node/ILA2 amplifier that amplifies DWDM channels transmitted to node/ILA1.
2. The Raman pumps in the two Raman amplifier packs that pump the spans will be completely shut down.

3. The OSC transmitter in node/ILA 1 will transmit a remote defect indicator (RDI) to node/ILA 2 and the OSC transmitter in node/ILA 2 will transmit an RDI to node/ILA 1.
4. Software will raise the `APR-Active-Line` condition against the outputs of the LD's with the gold-colored amplifiers, and against the LINE IN ports of both Raman amplifier packs.

Restart after repair of a double fiber cut

When the fibers that carry traffic between Node 1 and Node 2 are repaired in the order indicated in the following illustration, the following procedure will take place: (Power is restored between ILAs following the same procedure.)

Figure 14-13 Double fiber restoration



1. After the first fiber is repaired, the OSC receiver at the incoming LD in Node 1 detects the OSC from node 2. This receiver detects the RDI from Node 2. The two nodes are now experiencing only a single fiber cut, similar to what was described previously in, [“Restart after repair of a single fiber cut”](#) (p. 14-38).
2. When the second fiber is repaired, the OSC receiver at the incoming LD in Node 2 detects the OSC from Node 1.
3. In response, the LD in Node 2 that amplifies the DWDM channels transmitted toward Node 1 is turned back on.
4. Also in response to detection of the OSC, the RDI is removed from the OSC that is transmitted from Node 2 to Node 1.
5. After the OSC without an RDI is detected at Node 1.
6. The amplifier in Node 1 that amplifies the DWDM channels transmitted toward Node 2 is turned back on.
7. The `APR-Active-Line` condition is cleared.

Other failures that result in APR

APR can lead to shutdowns in certain cases when the span has not been cut. In these cases, APR may occur as a by-product of a failure. If a failure other than a span cut or disconnection leads to an APR shutdown, transmission will restart automatically using the standard restart procedure.

The following are examples of failures that may cause an APR shutdown:

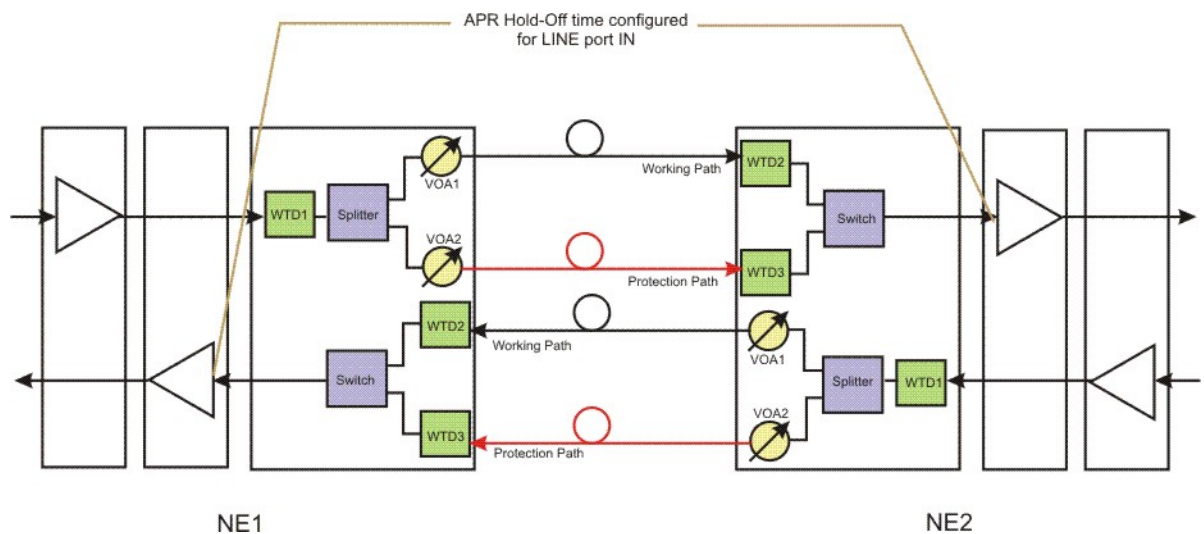
- A Raman amplifier is being used at a node or ILA, and the fiber is disconnected between the Raman amplifier and the ingress amplifier.
- A booster amplifier is being used at the node or ILA, and the fiber is disconnected between the booster amplifier and the egress amplifier.
- An OSC transmitter failure at one node or ILA leads to the shutdown of a Raman card at an adjacent node or ILA. If the channel count is small, the shutdown of the Raman card can result in DWDM LOS, in addition to OSC failure, at the ingress OA.

APR examples in OLP configurations

In an OLP configuration, the LD receiving the WDM signal from the line through the OPSA pack requires the capability to hold-off initiating Automatic Power Reduction (APR) signaling to the upstream line. The hold-off allows the OPSA to complete a switch in the case of a span break. The hold-off time must be long enough to allow the OPSA to complete its switch and for the LOS state to clear at the receiving LD. In a case where both working and protection paths between NE degrees are broken, normal line APR actions will occur after the hold-off time. Node APR must also be held off long enough to allow the OPSA to complete its switch. Since node APR is also based on measurement of total power, both line APR and node APR can be delayed by delaying report of DWDM LOS defects

In a node with OLP protection on a line, APR hold-off time is applied to the ingress LD receiving the line through the OLP-mode OPSA. The timer value is configured automatically when the LD topology is connected to the SIG port of an OPSA in OLP protection mode.

Figure 14-14 OLP example configuration



When a DWDM LOS is detected at the ingress LD LINE port, the pack will perform a recheck for the DWDM LOS after the APR hold-off time. If the LOS still exists, the pack will declare the LOS defect and, if correlation with OSC defects and OSC equipage indicates a port LOS, a port LOS defect is sent to the Equipment Controller. If the DWDM LOS is not present after the hold-off time, (or does not persist throughout the hold-off period) then the pack does not declare a port LOS defect. In that case the network element will not proceed to consequent APR actions and transmission will not be interrupted by the APR mechanism.

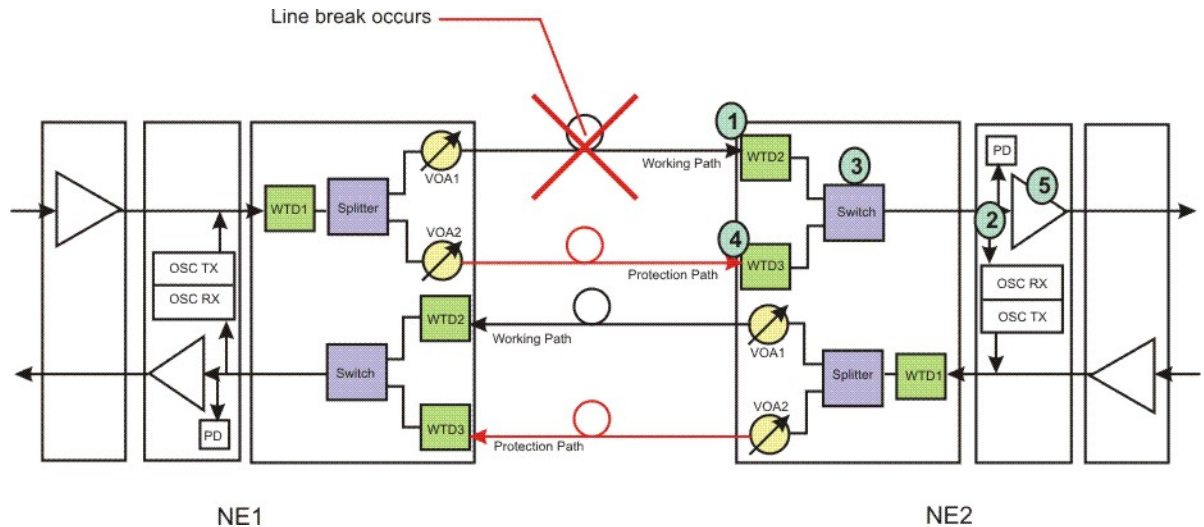
APR behavior for OLP with one branch of a protected span broken

If both working and protection spans of a line between an upstream network element (NE1) and a downstream network element (NE2) is protected by OLP are intact, the following sequence is expected when the working span (selected by the OPSA of NE2) is broken.

1. The OPSA A or B port will measure a loss of optical power.
2. Near simultaneously with OPSA detection, the ingress LD will measure the loss of DWDM and OSC signals. The ingress LD then begins counting the APR hold-off timer time duration.
3. The OPSA pack completes a switch to the protection span (B or A port). The working path is in signal fail state.
4. Transmission is established through the protection span.
5. The ingress LD measures recovery of the incoming DWDM signal above the LOS threshold, and the OSC LOS clears. Because the DWDM LOS does not persist for the duration of the APR hold-off timer; APR signaling from the downstream NE2 to the upstream NE1 is not initiated.

Note: Insertion loss results in a transmit level from NE1 onto the fiber that is lower than class 1M.

Figure 14-15 APR for OLP with single broken branch on a protected span

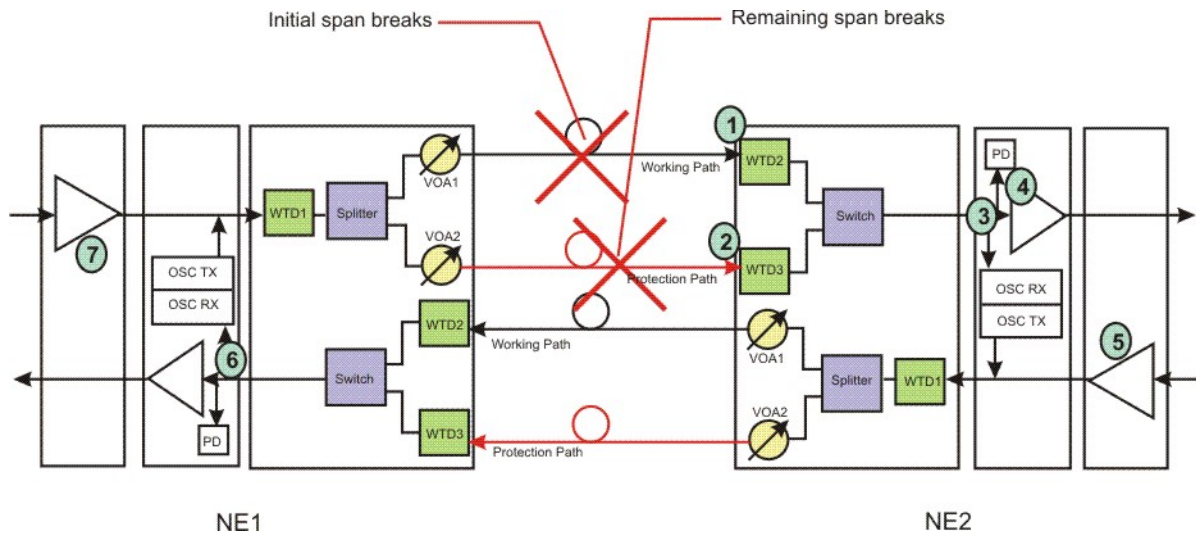


APR behavior for OLP with working and protection branches of a protected span broken

If one of the working/protection spans between an upstream network element (NE1) and a downstream network element (NE2) of a line protected by OLP fails due to a fiber break or high attenuation, the following sequence will occur when the remaining span (selected by the OPSA of NE2) is broken. Note that, if there is no upstream ILA LD, or OADM degree egress LD, transmitting to NE2, no upstream LD will need to be disabled.

1. The working path is in signal fail state.
2. When the fiber span is broken in the protection path, the OPSA protecting the line for NE2 will measure a loss of optical power.
3. Near simultaneously with OPSA detection, the ingress LD will measure the loss of DWDM and OSC signals. The ingress LD then begins counting the APR hold-off timer time duration.
4. After the end of the APR hold-off timer time duration, the DWDM signal condition is still LOS. The ingress LD raises DWDM LOS and OSC LOS defects correlating to the port LOS for the LINE port. (The OSC is considered failed for LOS, LOL, or LOF conditions.)
5. APR turns off the Egress LD in NE2 on the same line as the detecting line transmitting to the NE1, and inserts a remote defect indicator (RDI) in the OSC overhead transmitted to NE1. The APR-Active-Line condition is raised against the output port of the shut-off LD.
6. The ingress LD facing the same span receives the RDI from NE2.
7. NE2 turns off the Egress LD transmitting from NE1 to NE2, and raises the APR-Active-Line condition against the output port of the shut-off LD.

Figure 14-16 APR for OLP with both branches of a protected span broken

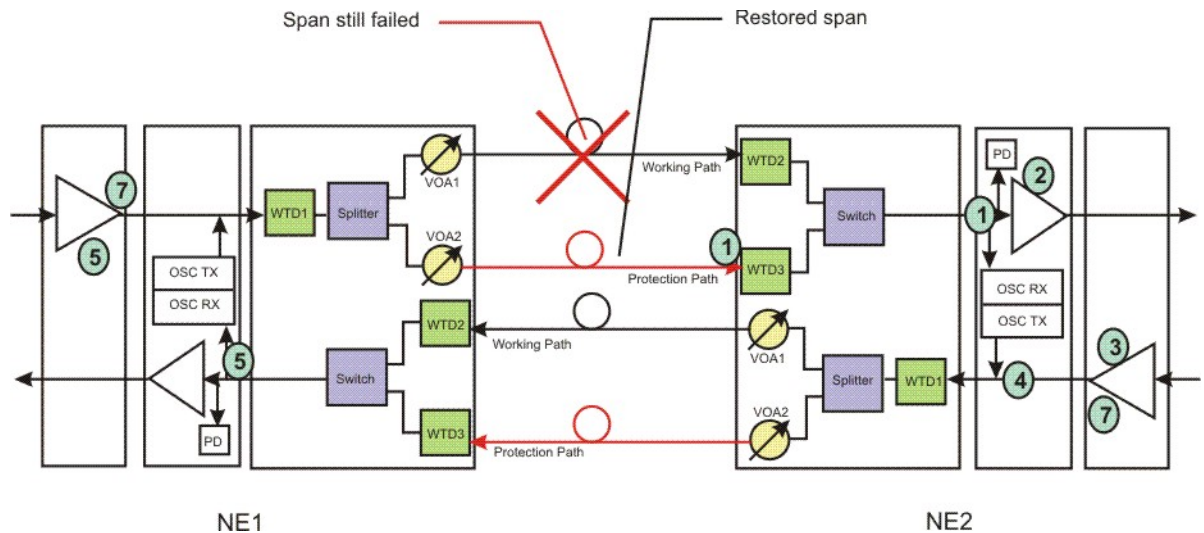


Restart behavior after restoring one path of broken working and protect paths

When a line is protected by OLP, if both the working and protection spans between an upstream network element (NE1) and a downstream network element (NE2) have failed due to a fiber break or high attenuation, the NEs are expected to be in the final state depicted in [Figure 14-17, “APR restart for OLP with single path restoration for broken span” \(p. 14-47\)](#). When the span presently selected by the OPSA switch is repaired, the following sequence is expected to restart transmission. Note that if there is no upstream ILA LD transmitting to NE2 or OADM degree egress LD transmitting to NE2, there is no upstream LD that needs to be re-enabled.

1. The DWDM LOS clears at the A|B In port of the NE2 OPSA. With the switch selecting the A|B port the DWDM LOS will clear at the ingress LD LINE port In and the OSC LOS, LOL and/or LOF defects will clear.
2. The ingress LD of NE2 will re-enable. (If it is a high power capable amplifier it will only enable to the eye-safe output level initially).
3. APR re-enables the egress LD (or ILA LD) transmitting from NE2 to NE1. (If it is a high power capable amplifier it will only enable to the eye-safe output level initially).
4. NE2 clears the RDI being sent back upstream to NE1 in the OSC overhead.
5. NE2 receives the RDI clear through the OSC and re-enables its egress LD (or ILA LD) transmitting towards NE2. (If it is a high power capable amplifier, it will only enable to the eye-safe output level initially).
6. (High power capable amplifiers clear node APR and enable at normal output power).
7. APR-Active-Line conditions clear for the re-enabled amplifiers.
8. (APR-Active-Node conditions clear for the re-enabled amplifiers, if applicable).

Figure 14-17 APR restart for OLP with single path restoration for broken span



OSCT card behavior

The OSCT cards do not provide full support for APR. They should not be used in configurations that include amplifiers with output powers that can exceed class 1M. OSCT cards may also not be suitable for use by customers that require APR shutdowns, even when safety standards can be met without APR.

If an OSCT card terminates an optical line, and the input fiber from the line to the OSCT card is cut or disconnected, the optical supervisory channel for the return path will not transmit the full set of RDI bytes back to the far end.

If there is a single-fiber cut, and if there is an egress amplifier that launches into the span at the far end, it will not shut down.

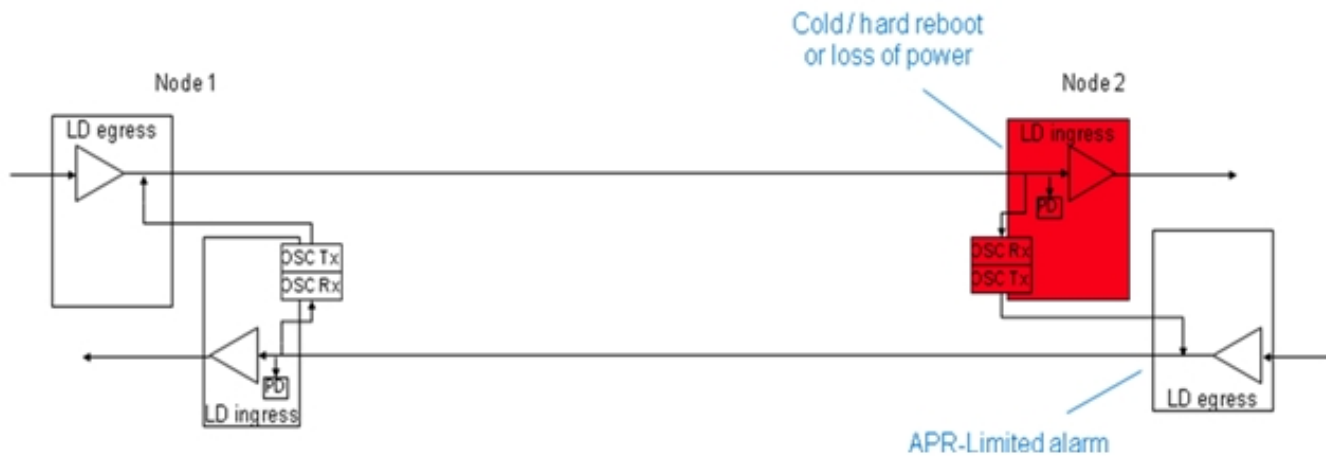
When there is a fiber cut, the OSCT card will detect the loss of signal for the supervisory channel and send out RDI-O back upstream. It will not, however, send back RDI-P, which indicates loss of the DWDM channels. Both RDI-O and RDI-P must be received at the upstream node or ILA in order to cause APR for a single fiber cut.

1830 APR with RAMAN and booster amplifiers

1830 PSS-32/PSS-16 can use Raman and high-power booster amplifiers as an option on long spans. These amplifiers have output power that exceeds the class 1M limits. So APR is required when these amplifiers are used. These amplifiers have their own internal APR algorithms, independent of NE software. The NE-based software is considered an essential addition to the booster's internal APR mechanisms.

APR behavior with LD reset or loss of power

Figure 14-18 Cold or hard reboot of a line-terminating LD



If a line terminating amplifier at a node that has an egress OA loses power or is subject to a cold or hard reboot, APR will not occur. However, an APR-Limited alarm will be raised against the output port of the egress LD.

Since `APRLINE` works bidirectionally, when an `APRLIMITED` alarm is raised against an egress LD, then APR could be unavailable for both directions of the affected optical line. In Figure 14-18, “Cold or hard reboot of a line-terminating LD” (p. 14-48), if a fiber cut occurs on the upper fiber, the ingress LD in node 1 will see OSC LOS, but not DWDM LOS. Thus the shutdown of the node 1 egress LD will be delayed until after the reboot of the node 2 ingress LD.

If the node is an ILA, then the egress LD is understood to mean the LD that launches into the return span. Referring to Figure 14-18, “Cold or hard reboot of a line-terminating LD” (p. 14-48), node 2 could be an ILA or a portion of an add/drop node. If the ingress amplifier in node 2 loses power or undergoes a cold or hard reboot, an APR-Limited alarm will be raised against the LineOut port of the egress LD in node 2.

When an LD that terminates a line has a cold or hard reboot, the OSC transmitter in the LD will remain off until the pack is fully booted, and the LD that launches into the return span will remain shut down. When rebooting has been completed, the OSC will transmit normally, with RDI being transmitted only if LOS conditions exist at the input to the LD.

If the line-terminating LD is a hybrid amplifier card, and the LD loses power or is cold or hard rebooted, APR will not occur. However, an APR-Limited alarm will be raised against the output port of the egress LD and against the LINE IN port of the ingress LD.

- A2325A
- AM2125A
- AM2125B
- AM2318A
- A2P2125
- AM2625A
- ASWG
- A4PSWG

14-49

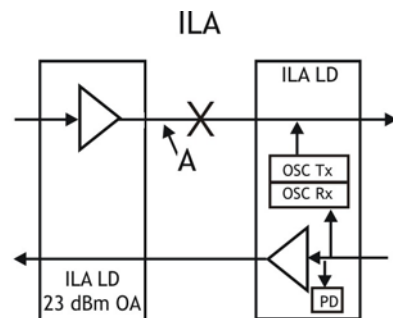
Fiber cuts and disconnects within a node or ILA

Eye-safe mode support

Note: The eye-safe level on most packs is at around 10 dBm. On some packs it could be at -2 dBm.

If the power level can exceed class 1M levels at point A in [Figure 14-20, “ILA fiber cut between OA’s exceeding class 1M limit”](#) (p. 14-50), the output power must be reduced if the connection is broken between the high power output of one port and the port that follows.

Figure 14-20 ILA fiber cut between OA's exceeding class 1M limit



If an A2325A LD is used in an ILA or as egress LD for a FOADM, ROADM, or TOADM node, fibered as shown in [Figure 14-20, “ILA fiber cut between OA’s exceeding class 1M limit”](#) (p. 14-50), power will be reduced within 3 seconds of a cut on the Sig Out port of the high power LD. The existence of the cut is determined by an LOS threshold at the Line Out port of the LD that follows the cut. The power will be reduced using the eye-safe output mode of the amplifier. The amplifier will exit eye-safe mode and restore full power after an LOS clearing threshold has been exceeded.

TOADM or ROADM ingress LD

If the power level can exceed class 1M levels at point A or at point B in [Figure 14-21, “Fiber cut after ingress LD”](#) (p. 14-51), output power must be reduced if the connection is broken between the high power output of one port and the port that follows.

Figure 14-21 Fiber cut after ingress LD

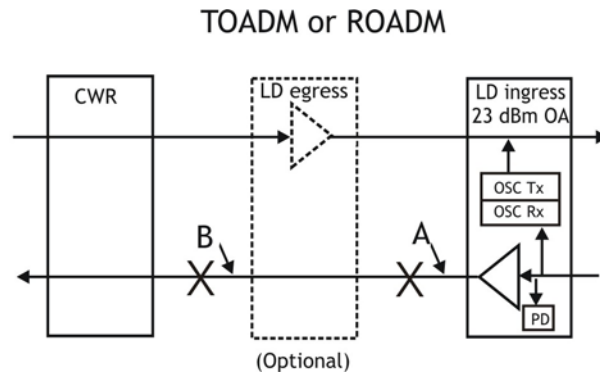
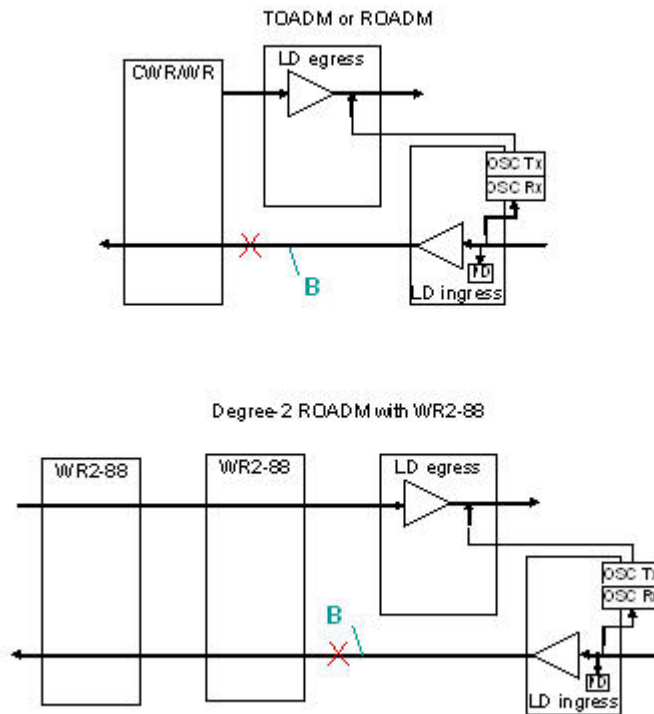


Figure 14-22 Fiber cut after unidirectional ingress LD



If an A2325A LD is used as an ingress LD at a TOADM or ROADM node, and an egress LD is present fibered as shown in [Figure 14-21, “Fiber cut after ingress LD”](#) (p. 14-51), output power will be reduced within 3 seconds when there is a cut after the Sig Out port of the high power LD. The existence of the cut will be determined by an LOS threshold at the Line Out port of the LD that follows the cut. The power will be reduced using the eye-safe output mode of the amplifier. The amplifier will exit eye-safe mode and restore full power after an LOS clearing threshold has been exceeded.

Note: The eye-safe level on most packs is at around 10 dBm. On some packs it could be at -2 dBm.

Topology download

Software validates the topology of the node or ILA. If the amplifier in the LD is capable of exceeding the class 1M safety limit, then the pumps on that amplifier will remain shut off until a valid topology has been provisioned. Until a valid topology has been received, an APR-Active-Invalid Topology condition will be raised. The amplifiers that are subject to this requirement are listed below.

- A2325A
- AM2625A
- A2P2125
- AM2125A
- AM2125B
- AM2318A
- ASWG
- A4PSWG

The APR-Active-Invalid Topology condition will also arise when partial topologies are downloaded, for example when only the internal connections within the ILA have been provisioned. In [Figure 14-20, “ILA fiber cut between OA’s exceeding class 1M limit” \(p. 14-50\)](#), where the LD on the left has a high-power amplifier, that amplifier must remain turned off with the APR-Active-Invalid Topology condition raised, until the external connection is provisioned at the LINE OUT port of the right-hand LD.

If a connection that is monitored for intranode APR is deleted, APR will result. The amplifier output power will be turned completely off, and the APR-Active-Invalid Topology condition will be raised.

Circuit pack failure or removal

For all pack failure cases, APR will occur if the cause of failure is detected on the failed pack itself. APR will also occur if the FpgaClkNotSync defect (EQPTDGR condition) is detected. The following exceptions apply:

- APR will not occur in the following cases:
 1. APR will not occur when a line-terminating LD at a node that has an egress OA fails or is removed. However, an `APR-Limited` alarm will be raised against the output port of the egress LD.
 2. APR will not occur when a line-terminating LD at a node that is preceded by an RA2P fails or is removed. However, an `APR-Limited` alarm will be raised against the LINE IN port of the RA2P. In addition, step 1 applies.
 3. APR will not occur when the failed/removed line-terminating LD at a node is a hybrid LD. However, an `APR-Limited` alarm will be raised against the LINE IN port of the hybrid LD. In addition, step 1 applies.
- If the ingress LD is an A2325A, and the egress LD fails or is removed, APR will not occur. However, an `APR-Limited` alarm will be raised against the SIG output port of the ingress A2325A.
- If a CWR or WR fails or is removed, and if the ingress LD that supplies power to the SIG IN port of the CWR or WR is a high-power amplifier (greater than class 1M power level), APR will not occur. However, an `APR-Limited` alarm will be raised against the output port of the ingress LD.
- APR will not occur when an RA2P fails. However, an `APR-Limited` alarm will be raised against the LINE IN port of the RA2P.

The Raman pumps will shut down and the `APR-Active-Line` condition will be raised against the LINE IN port of the Raman amplifier. There is no attempt to pulse the Raman pumps of a failed Raman amplifier pack in this case.

- If a WR8-88A or WR8-88AF in an anydirection add/drop block fails or is removed, and if the ingress LD that supplies power to the SIG IN port of the WR is a high-power amplifier (greater than class 1M power level), APR will not occur. However, an `APR-Limited` alarm will be raised against the output port of the LD.

Forced APR

For ASWG and A4PSWG cards a forced APR capability is integrated in the APR software. This allows the amplifiers to be shut down even when they have optical cross-connects. Forced APR may be used on the LineOut port to shut down the EDFA outputs of ASWG and A4PSWG, and on the LineIn port of A4PSWG to shut down the Raman amplifier.

Forced APR may be used to perform out-of-service OTDR scans. Ordinarily, APR recovery occurs automatically when a fiber span is repaired, but automatic restart is prevented by forcing APR. When the out of service OTDR scan has been completed, the forced APR condition can be removed, so that automatic restart of the line can occur.

Extreme care must be taken when using forced APR, since it will shut down traffic. Administrative-level privileges are required to use forced APR, and an APR Forced alarm is raised.

Disabling APR

Automatic power reduction (APR) will be performed on egress amplifiers at 1830 add/drop nodes, and at ILA's in response to a fiber span cut or disconnection. APR is required by safety standards if the output power of the amplifier can exceed the class 1M limit. A functioning Optical Supervisory Channel (OSC) is normally required to clear an APR-Line condition and allow egress amplifiers to start up or restart. For some long spans, it is necessary to operate without an OSC in order to overcome reach limitations. For these spans, APR must be disabled.

Disabling of APR is restricted to egress LDs whose optical amplifiers fall within the class 1M limit.

A user can disable APR on an egress LD at a node, or at an LD at an ILA, provided that the egress LD is one of the following:

- AHPHG
- AHPLG
- ALPHG

APR may also be disabled on the egress amplifiers within the following cards:

- IROADMF
- IROADMV

It is not possible to disable APR on any circuit pack that is not listed in this requirement, or to disable amplifiers that are used as ingress amplifiers at add/drop nodes or DGEs. APR is enabled by default. If APR is disabled, it is possible to re-enable the same.

If APR has been disabled at the egress LD of a node or ILA, and if the egress LD has been shut down for an APR condition, then the optical amplifier in the LD shall restart even if there is an OSC LOS condition at the ingress LD of the same node/ILA. The restoration of power is subject to the 100 second delay that is described in the APR overview. In addition, if the LD has undergone a cold or hard reboot, then the amplifier shall restart even if there is an OSC LOS condition at the ingress LD of the same node/ILA.

Optical transponders

Supported OTs

In Release 8.2 the Alcatel-Lucent 1830 PSS supports the following OTs for WDM compounds. Not all OTs are supported on all shelf-types. For details about specific shelf and slot support for individual OTs, see [“Alcatel-Lucent 1830 PSS racks, subracks, common parts, cards, and other mechanical items”](#) (p. 18-5).

- 4DPA4: MSC - 4G Dual Port Pluggable AnyRate (4 client)
- 4DPA2: 4G Dual Port Pluggable AnyRate (2 client)
- 11STAR1: 11G Single Port Tunable AnyRate (1 client)
- 11STAR1A: 10G OT, enhanced (backward compatible to 11STAR1)
- 11STGE12: 11G Single Port Tunable GBE Mux (12 client)
- 11STMM10: 11G Single Port Tunable Multirate Mux (10 universal clients)
- 11DPM8: 11G 8 x Any Add-drop Optical Transponder
- 11DPM12: 11G Dual Port Pluggable Multirate Mux (12 universal clients)
- 11DPE12: 11G Dual Port Pluggable GBE Mux (12 client)
- 11DPE12E: 11G Dual Port Pluggable GBE Mux, Enhanced
- 11DPE12A: 11G Dual Port Pluggable GBE Mux, Enhanced - next generation
- 11QPA4: 11G Quad Port Pluggable Anyrate (4 client)
- 11QPA4A: 11G Quad Port Pluggable Anyrate HARDENED (4 client)
- 11QPE24: 11G/10G Quad + 24GE/FE Interface Board
- 11QCE12X: 11G/10GE Quad Interface
- 11QPEN4: 11G Quad Port Pluggable SAN Encryption
- 43STA1P: 43G Single Port Tunable Anyrate (1 client) - optimized for 88 channels, C-band, PDPSK
- 43STA1PB: 43G Single Port Tunable Anyrate (1 client) - optimized for 88 channels, C-band, PDPSK (Enhanced)
- 43SCA1: 43G Single Port Tunable AnyRate Coherent (1 client) A/D, MSA, 16ps
- 43STX4: 43G Single Port Tunable Mux (4 client), optimized for 44ch in C-band, DPSK
- 43STX4P: 43G Single Port Tunable Mux (4 client), optimized for 88ch in C-band, PDPSK
- 43SCGE1: 40GbE SPT Coherent A/D (client CFP)
- 43SCX4: 40G Single Port Tunable Mux Coherent (4 client)
- 43SCX4E: 40G Single Port Tunable Mux Coherent (4 client), 2 slot
- 112SCX10: 100G Single port tunable mux (10 universal clients), coherent
- 112SNX10 : 10x10G Mux, Coherent w/Enh OSNR

-
- 112SCA1: 100G anyrate A/D, Coherent
 - 112SNA1: 100G Anyrate A/D, Coherent w/Enh OSNR
 - 112SDX11: 112G DCI High capacity muxponder (11 clients)
 - 130SCX10: 10x10G SDFEC Muxponder
 - 130SNX10: 10x10G SDFEC Muxponder supporting FlexGrid
 - 130SNQ10: 130G Single Port Tunable AnyRate Transponder - 10 clients
 - 130SCA1: 100G Add/Drop OT (1x100G) with SDFEC (2 slot)
 - 260SCX2: 2x100G Transponder/Muxponder card
 - 1UD200: 100/200G Uplink Dist OTN Switch
 - 20P200: 20x10G Multirate I/O Module
 - D5X500: 500G Mux/uplink

WDM Protection

Supported WDM Protection

Several types of OT and link protection supported for Alcatel-Lucent 1830 PSS/PSS-4 WDM compounds are described in this document, including the following.

- OPS
- OMSP
- E-SNCP
- Y-cable/O-SNCP
- LAG
- OLP

Details about components and configurations supported for each of these can be found in [“Protection configurations” \(p. 17-117\)](#).

OAM&P features

Overview

Purpose

This section provides information features related to OAM&P for WDM applications of Alcatel-Lucent 1830 PSS.

Contents

Operation, administration, and maintenance	14-60
Wavelength Tracker	14-68
Alien wavelengths	14-79

Operation, administration, and maintenance

Management interfaces

The Alcatel-Lucent 1830 PSS NE supports a range of management interfaces:

- Simple network management protocol (SNMP)
- Transaction language 1 (TL1)
- WebUI interface
- Command line interface (CLI)

Simple network management protocol (SNMP)

The Alcatel-Lucent 1830 PSS system supports the following SNMP functions:

- Provisioning interface for all equipment and parameters through SNMPv3.
- Reporting of all alarms/traps and ability to define trap destination.

Transaction language 1 (TL1)

The Alcatel-Lucent 1830 PSS system supports a TL1 command interface for all provisioning, reporting, and alarming.

WebUI interface

The Alcatel-Lucent 1830 PSS network element (NE) includes a web server so that craft can manage an NE from any Windows-based PC with a web browser, without the need for any other special software.

WebUI software requirements

The WebUI supports the following versions of PC software:

- Windows 7 and Windows 8
- Internet Explorer 11.0
- MAC OS 10.9 (with Firefox browser only)
- Firefox 38ESR and 41

The following functionality is not supported with the Firefox browser:

- Show in separate window
- Export to Excel
- Launching JDSU viewer for viewing OTDR scan results

Note: Beginning with Release 8.1, J2SE Java Runtime Environment (JRE) is no longer used by the WebUI.

Command line interface (CLI)

A CLI supports all Alcatel-Lucent 1830 PSS, PSS-4 system functionality.

A CLI supporting GMPLS is also available, but should be used as a debug interface, or for local access. By default, GMPLS networks are managed by a network management system (NMS).

Gateway network element (GNE)

The network management system can manage an Alcatel-Lucent 1830 PSS network while only connecting to a single NE. That NE is called a GNE and provides the management connectivity to all other 1830 PSS-32 and 1830 PSS-16 NEs in the network.

Optical supervisory channel (OSC) inter-node communication

The OSC is a separate optical channel, operating at the STM-1/OC-3 rate of 155 Mb/s, that transfers management and control information between the ECs of two adjacent nodes, regardless of whether any of the DWDM payload channels are terminated between those two nodes. The channel is capable of transporting both IP and OSI PDUs.

General communications channel (GCC) inter-node communication

OSC is not available in CWDM transmission, so the GCC is used for inter-node communication.

GCC0

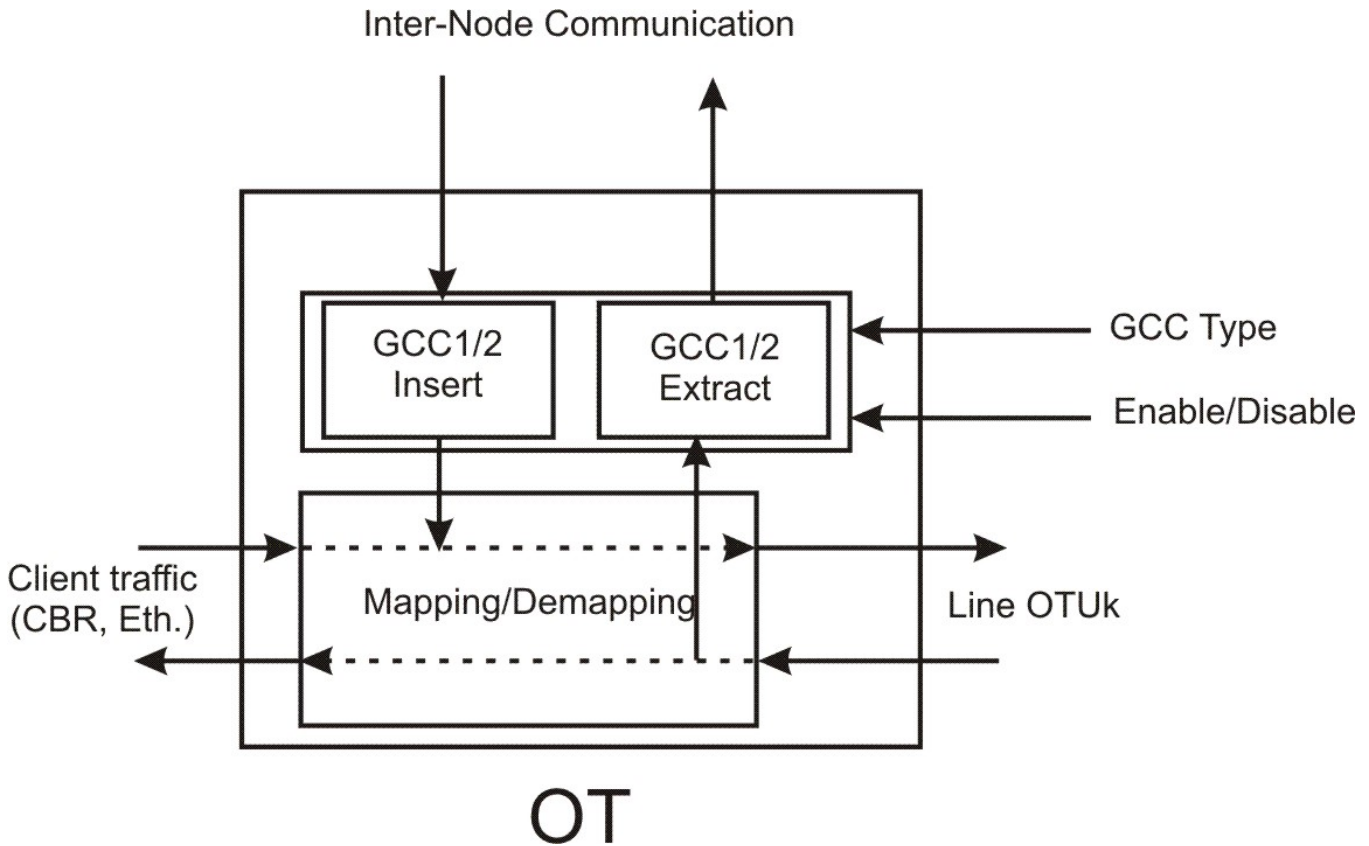
All OT packs with a OTUk signal interface terminate the OTUk GCC0 channel.

When the GCC0 channel is disabled, communication information is not transmitted over the GCC0 channel. In the transmitting direction, the GCC0 bytes are set to all zeros, and in the receiving direction, the GCC0 is ignored and the GCC data link is disabled.

GCC1/GCC2

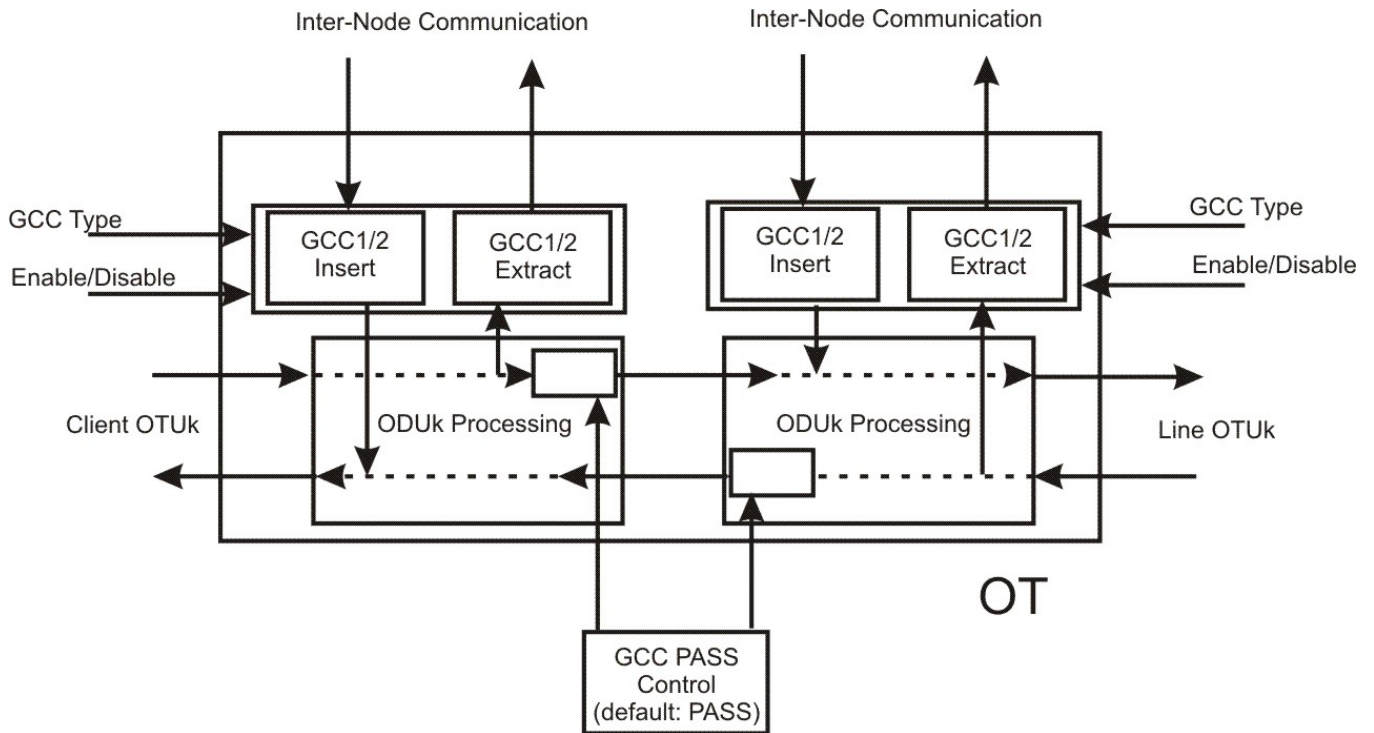
Two types of COMMS functions are defined for the communication channel within ODUk layer:

- ODUkp Termination Mode: The GCC1/GCC2 overhead is inserted/extracted at the ODUkp access point. This function is applied to OT's Line port with OTUk interface carrying the CBR/Ethernet clients.



This mode is applied to the following OT ports:

- 11QPA4(A) Line port with non-OTU2 client signal (OC-192, 10GbE, 10GFC)
- 11STAR1 Line port with non-OTU2 client signal (OC-192, 10GbE, 10GFC)
- 43STX4(p) Line port with all types of client signals
- 43STA1P(B) Line port with OC-768 client
- 11DPM8 Line port with all types of client signals
- 11DPM12 Line port with all types of client signals
- 11DPE12E Line port
- 11QPE24 Line port
- 11DPE12A Line port
- **ODUk Regeneration Mode:** The GCC1/GCC2 overhead is inserted/extracted at the connection point of one ODUk with another ODUk. This function is applied to the OT's Line/Client port with the interface in the configuration of the OTUk regeneration.



The GCC functions in OTUk regeneration model are applied to the following OT ports:

- 11QPA4(A) Line Port with OTU2 Client signal
- 11QPA4(A) Line Port in Cross-Regen mode
- 11STAR1 Line/Client port with OTU2 Client signal
- 43STA1P Line port with OTU3 Client
- 11STMM12 Client port with OTU1 Client

GCC0/GCC1/GCC2 provisioning

The following OTs shall support GCC0/GCC1/GCC2 type provision:

- 11STAR1 Line/Client port
- 11QPA4(A) Line port
- 11DPE12E Line port
- 11DPM8 Line port
- 11DPM12 Line port
- 43STX4P Line/Client port
- 43STA1P Line/Client port

GCC MTU value

The default GCC MTU value has changed in R7.0 from previous releases to "1500 bytes" for all associated packs/ports. Any new GCC connection added between two NEs running Release 7.0 or greater and an earlier release will not automatically come up unless the user ensures the provisioned MTU value matches on both sides of the connection.

GCC packet type

The GCC packet type is only provisionable for the following packs:

- 11STAR1
- 11DPE12E
- 4DPA4
- 11STMM10

Note: GCC packet type should always be set to standard. Any new GCC connection added between two NEs running Release 7.0 or greater and an earlier release will not automatically come up unless the user ensures the provisioned GCC packet type value matches on both sides of the connection.

Management resiliency

Duplex equipment controllers

An 1830 PSS-32 or 1830 PSS-16 node can be provisioned with a single EC or with duplex EC for 1+1 redundancy. nodes. With duplex controllers, a failure of the main controller will cause an automatic protection switch to the backup controller. In either case, a controller failure does not affect transmission or service availability.

Multiple gateway NEs

More than one NE in an 1830 PSS network can be designated to be a GNE. In this way, management connectivity can be maintained in the event of DCN and/or 1830 PSS NE failures.

Redundant optical supervisory channel

For ring and collapsed ring topologies, OSC communications to all nodes will be maintained in the event of a fiber break on any single span.

Performance monitoring

The Alcatel-Lucent 1830 PSS supports Performance monitoring on 100 percent of all points of termination and adaptation on the boundaries of the system and between subsystems.

Optical PM

The system supports the monitoring and reporting of received and transmitted optical power on client and DWDM line-side interfaces.

OTN

The line signal is G.709-framed and the Alcatel-Lucent 1830 PSS monitors the section and path performance parameters shown in [Table 14-6, “OTN performance monitoring” \(p. 14-65\)](#).

Table 14-6 OTN performance monitoring

PM parameter	Section	Path
Errored seconds (ES)	Yes	Yes
Severely errored seconds (SES)	Yes	Yes
Unavailable (UAS)	Yes	Yes
Background block errors (BBE)	Yes	Yes
FEC: corrected bits	Yes	NA
FEC: uncorrected bytes	Yes	NA

Performance monitoring complies to ITU-T G.874 and G.798.

SDH/SONET client

The B1 and B2 overhead bytes are monitored. There are counters for code violations (CV), ES, SES, and severely errored framing seconds (SEFS).

Ethernet client

The Alcatel-Lucent 1830 PSS supports the non-intrusive monitoring of Ethernet per RFC-2819, including ingress counters for CV, valid bytes and valid frames, and a wide array of RMON performance monitoring statistics.

Fibre channel client

The Alcatel-Lucent 1830 PSS counts ingress code violations.

Optical supervisory channel digital PMs

The 1830 PSS-32 and PSS-16 support the monitoring and reporting of these OSC PMs: CV and BBE.

Fault management

The Alcatel-Lucent 1830 PSS is provisionable on a per-port basis to detect/process, and report faults, failures, and performance. It is able to diagnose equipment faults down to a field replaceable unit (FRU) or interface. Transport fault processing is performed as defined in G.783 and EN 300 417. The system allows provisioning for the SONET-specific LOS/LOF handling to satisfy Telcordia GR-253 issue 3 (2000) and ANSI T1.231.

There is one system default alarm profile that contains all alarms/conditions supported in the system and their severity: Critical, Major, Minor. The user can change the severity of alarms on each port/facility independently or point to the system profile. The system profile can be modified or reset to factory defaults

Optical line

Optical line fault processing is supported.

OTN

The Alcatel-Lucent 1830 PSS complies to G.709 for defect/fault processing of OTUk/ODUk overhead at all OTUk/ODUk interfaces.

The following is a short summary of the main functions of the OTN.

- Loss of frame (LOF) detected, causes signal fail (SF) condition and Alarm Insertion Signal (AIS) insertion.
- Source and Destination Access Point Identifiers (SAPI and DAPI) are monitored. When trail Trace Identifier Mismatch (TIM) is detected, it causes a signal fail (SF) condition and AIS insertion.
- Bit-interleaved parity (BIP-8) is inserted at the source. When parity violations are detected, indicating that the signal has degraded, a backward error indication (BEI) is inserted on the return to the source.
- The OTN checks for error conditions and inserts the following when appropriate: AIS, Incoming Alignment Error (IAE), Backward Incoming Alignment Error Indication (BIAE), and Backward Defect Information (BDI).

SDH/SONET

The Alcatel-Lucent 1830 PSS complies to G.707 and GR-253 for defect/fault processing at all STM-n/VC-m and OC-n/STS-m interfaces, respectively. For transparent transport of these client signals, the Alcatel-Lucent 1830 PSS supports non-intrusive monitoring in the source and sink directions.

The following is a short summary of the main functions.

- A1, A2 bytes monitored; LOF declared when appropriate
- B1 bytes monitored; degraded signal conditions declared when appropriate
- J0 byte monitored; TIM and SF declared when appropriate

CLAN

Physical on-site LAN connections are supported by the RJ-45 network connections (E1/2, ES1/2, VOIP, and so on.) on 1830 PSS-32/PSS-16 administrative modules. This LAN can be extended to other NEs over CLAN: a virtual LAN whereby the 1830 PSS-32/PSS-16 network transports LAN traffic between NEs, over the OSC. The physical on-site LAN is connected to CLAN using the LAN interface of an optical amplifier.

CLAN includes the following capabilities and behaviors.

- Enabled by default
- Disabled when OSC is configured as 100BASE-FX
- Auto-negotiation for 10/100 speed
- MDI/X auto-sensing and duplex (half/full)
- Transport of externally tagged packets

Currently, CLAN has the following limitations.

- Not functional (disabled) when OSC mode is configured as 100BASE-FX (100 Mbps)
- QoS to guarantee traffic quality is not currently supported
- Alarm and performance monitoring for the OT LAN (CLAN) connection, and port status (up/down) is not currently supported
- Ability to prioritize the customer LAN traffic differently over OSC from UPSR traffic is not currently supported

Wavelength Tracker

Overview

Carriers need tools for managing the WDM layer that are similar in effectiveness to those at the SDH/SONET layer. The Alcatel-Lucent 1830 PSS has been designed with a unique Wavelength Tracker capability, which enables every wavelength to be traced as it passes through the WDM network.

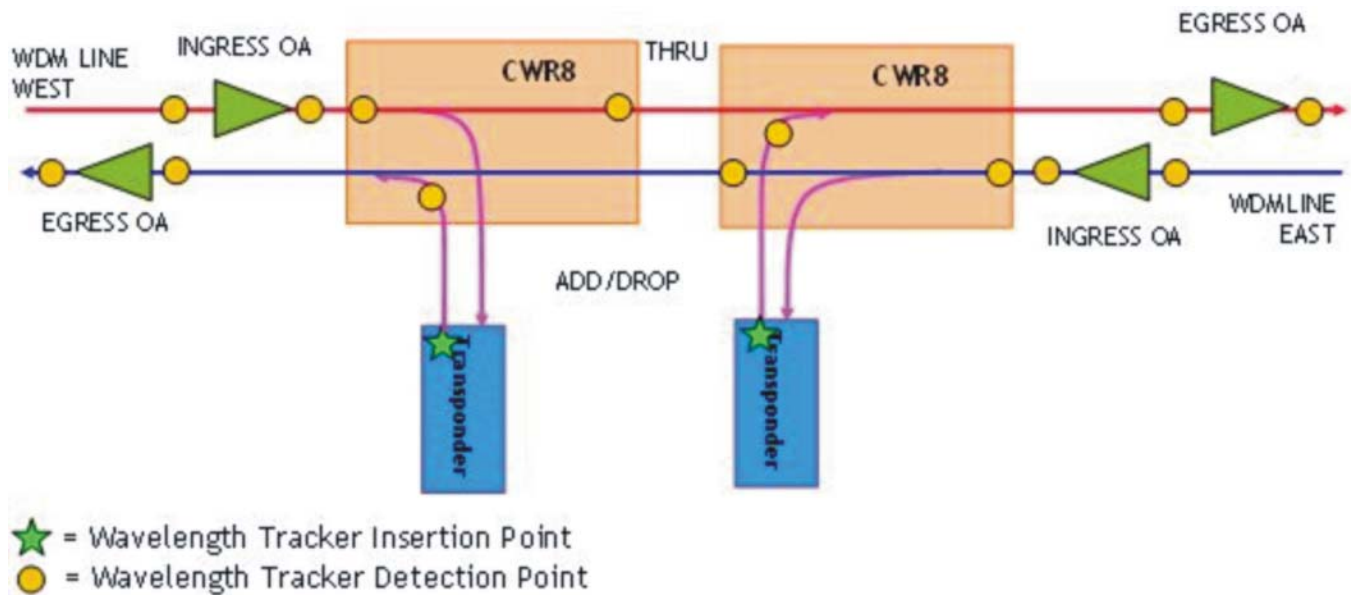
How Wavelength Tracker works

Wavelength Tracker architecture is based on the principle of “encode once, decode many times”. It uses a unique optical signature known as a “WaveKey” pair, which is encoded into each service wavelength at the transponder’s transmitter before it enters the WDM layer. Combinations of keys that create these signatures can provide up to 113 signatures per OCh frequency supported by the system. Bidirectional services use a WaveKey pair per direction; therefore 56 bidirectional services are possible from the Wave Key signature pool per OCh frequency.

Optical taps and DSP-based WaveKey decoders in optical modules throughout the optical network, and in dedicated Wavelength Tracker Optical Channel Monitors (WTOCM/WTOCMAs in Alcatel-Lucent 1830 PSS-32/Alcatel-Lucent 1830 PSS-16) on long-haul spans, “read” the WaveKeys. These units can provide the optical power level for each wavelength, allowing complete optical layer visibility for network fiber connectivity and faults at multiple points in each NE, regardless of whether the wavelengths are added, dropped, or simply passed through. Wavelength tracker decoding (WTD) is supported on all Alcatel-Lucent 1830 PSS Line Drivers (LD), CWR & WR packs, and OPSA. The OPSB does not support WTD detection.

Refer to [Figure 14-23, “Wavelength Tracker coding and encoding points”](#) (p. 14-69).

Figure 14-23 Wavelength Tracker coding and encoding points



The key to Wavelength Tracker’s cost-effectiveness is that it accomplishes all this totally within the optical domain. Therefore, no expensive optical-to-electrical-to-optical (O-E-O) conversions or optical spectrum analyzers are needed, reducing overall system cost.

The assignment of WaveKeys is managed by the network elements (NEs), which maintain a database of the WaveKeys used in the network.

Legacy wavekey scalability

Prior to Release 6.0.6, when more than 113 Wavelength Tracker key pairs are needed in a network per optical channel frequency, key reuse is possible if the network has isolated pockets of NEs. The isolated NEs can form a separate optical domain, which can be managed as a separate network. The OAMP port of one of the NEs in this separate network is used to provide the management interface to the network. The pool of 113 WaveKey pairs is then available again within the separate network. Each separate area can be assigned a different OSPF area number.

Wavekey scalability enhancements

Wavekey scalability enhancements provide support for reusing Wavelength Tracker key signatures within a single optical network in the same OSPF area. This provides increased flexibility for Wavelength Tracking in networks that evolve over time to require more than 56 bidirectional services of the same channel frequency within a domain. Conflicts

caused by key-pair duplication when two networks are joined together into a single network sharing an OSPF area can be resolved by selectively allowing duplicate keys within a domain.

The NE supports reuse of Wavelength Tracker key pairs for trail instances. The capability for the network to reuse Wavelength Tracker key pairs is enabled on a per OCh frequency basis, therefore it is possible to permit duplicates usage for some channel frequencies while reserving exclusivity for other channel frequencies. A network operator need only provision one service of a given OCh frequency with Wave Key duplicates allowed, or initiate a rekey with duplicates allowed operation on an existing service, in order to enable reuse of Wave Key duplicates for future instances of that OCh frequency.

The rekey with duplicates allowed capability allows an operator to clear a key duplicate alarm from a network.

New alarms are associated with this feature.

- A new WT encoder port condition is used to indicate if no keys can be selected given the rules for auto keying that apply to the channel being keyed. This condition can be used by an operator to understand that all possible Wave Key combinations have been assigned for the OCh frequency of the channel, and rekeying with duplicates allowed is necessary for key selection.
- A new cross-connect end-point condition used to indicate if two instances of the same WT keys are provisioned on the same node. This condition is informational only and has a severity of not alarmed. The information is provided in case a network operator wants to minimize the amount of key reuse on a single NE.

The system supports hitless upgrade to Release 7.0.0 with the WT Key scalability enhancements. While the network is in the process of being upgraded nodes of mixed release number may coexist. WT keying supporting service provisioning and deletion will still work in this context. Making use of the ability to reuse Wave Key pairs is not recommended until the network is completely software upgraded.

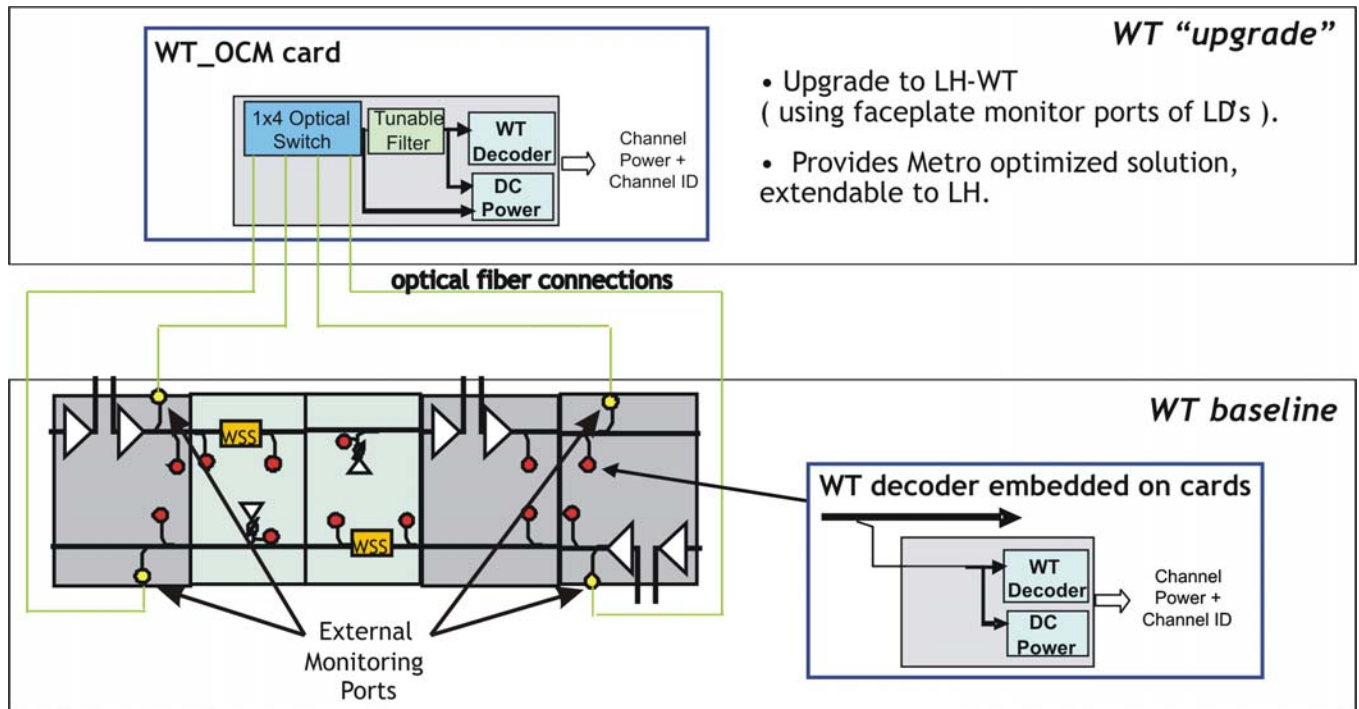
For specific information on alarms supporting the Wavekey scalability enhancements, see the *Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 8.2 Maintenance and Trouble-Clearing Guide*. For specific provisioning information, see *Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 8.2 User Provisioning Guide*.

Long haul Wavelength Tracker

The Alcatel-Lucent 1830 PSS supports both “standard” Wavelength Tracker (WT), for regional applications, and Long-Haul Wavelength Tracker (LH-WT), for long haul applications. LH-WT is supported by the WTOCM/WTOCMA card, which is connected to the external facing LD on an optical line, as shown in the figure below. In long-haul applications with the presence of SRS (stimulated RAMAN scattering) Wavelength Tracker WTOCM/WTOCMA is required to accurately control power levels.

The following figure shows how a WTOCM/WTOCMA card is connected to a module to enhance embedded baseline Wavelength Tracker capabilities for long-haul application.

Figure 14-24 WTOCM/WTOCMA addition for long haul WT



The WTOCM/WTOCMA is supported with the following LDs:

- A2325A
- AM2032A
- AM2625A
- AHPHG
- AHPLG
- ALPHG
- AM2125A
- A2P2125
- AM2125B
- AM2318A
- RA2P

(RA2P equipped lines can be monitored with WTOCM/WTOCMA; the WTOCM/WTOCMA connects to the EDFA LD following the RA2P).

Each WTOCM/WTOCMA can provide LH-WT for any two LDs.

Each line within an optical node, and each endpoint on an OMS span, must be configured with the same WT capability, either long haul (with WTOCM/WTOCMA), or standard (without WTOCM/WTOCMA).

An unkeyed optical channel is supported by WTOCM/WTOCMA on an auto-power managed line for the following node types:

An unkeyed optical channel is supported by WTOCM/WTOCMA on auto-power managed lines in long haul configurations for the following node types:

- ILA
- TOADM
- FOADM end-terminal with DGE in path

The WTOCM/WTOCMA is optional for the following node types:

- 2D+FOADM
- FOADM end-terminal, with no DGE in path

WT to WTOCM/WTOCMA network upgrade

One of three reasons could indicate the need to deploy the WTOCM/WTOCMA packs in a network:

- The EPT analysis of the network indicates that WTOCM/WTOCMA packs are required to provide sufficiently accurate power measurements to minimize transmission penalty from inaccurate power settings.

As the distance reach of the network and channel count of the network increases, the Stimulated Raman Scattering limit of detection by embedded Wavelength Tracker detectors may be reached.

- In anticipation of the previous scenario, it may be advantageous to take advantage of an opportunity to add WTOCM/WTOCMA packs to the network.
- There may be a need to take advantage of new features offered only with WTOCM/WTOCMA equipped networks.

In all cases a switch-over from WTD-only monitored network to a WTOCM/WTOCMA monitored network must be done carefully. When the switch is made, per channel power levels used by the system will shift. Optical power level control loops must react to the new power levels, therefore a phased approach to WTOCM/WTOCMA rollout is required. Within each phase time must be allocated to allow for power level settling. The procedure for an in-service upgrade to WTOCM/WTOCMA is detailed in Appendix C of the *Alcatel-Lucent 1830 Photonic Service Switch 16/32 (PSS-16/PSS-32) Release 8.2 Installation and System Turn-Up Guide*, ISSUE 2. Failure to follow this procedure could result in impacts to services.

Applications

Wavelength Tracker includes several applications.

Wavelength path trace

The WaveKey acts as an “Optical J0” Trace identifier. Wavelength Tracker traces the end-to-end path of each wavelength, distinguishing each from all other wavelengths—even multiple instances of the same wavelength when wavelength reuse is employed on a network.

Optical power management

In ROADM/TOADM systems, power management is fully automated. Target optical power levels are calculated for critical points in the system. Actual per-channel optical power is measured by Wavelength Tracker. Algorithms then feed back to control power at the transponder transmitter and at the wavelength router (CWR8/CWR8-88/WR8-88A/WR8-88AF/WR2-88) . (On the former, a variable optical attenuator [VOA] is used; on the latter, the power control is built-in to the optical switching fabric).

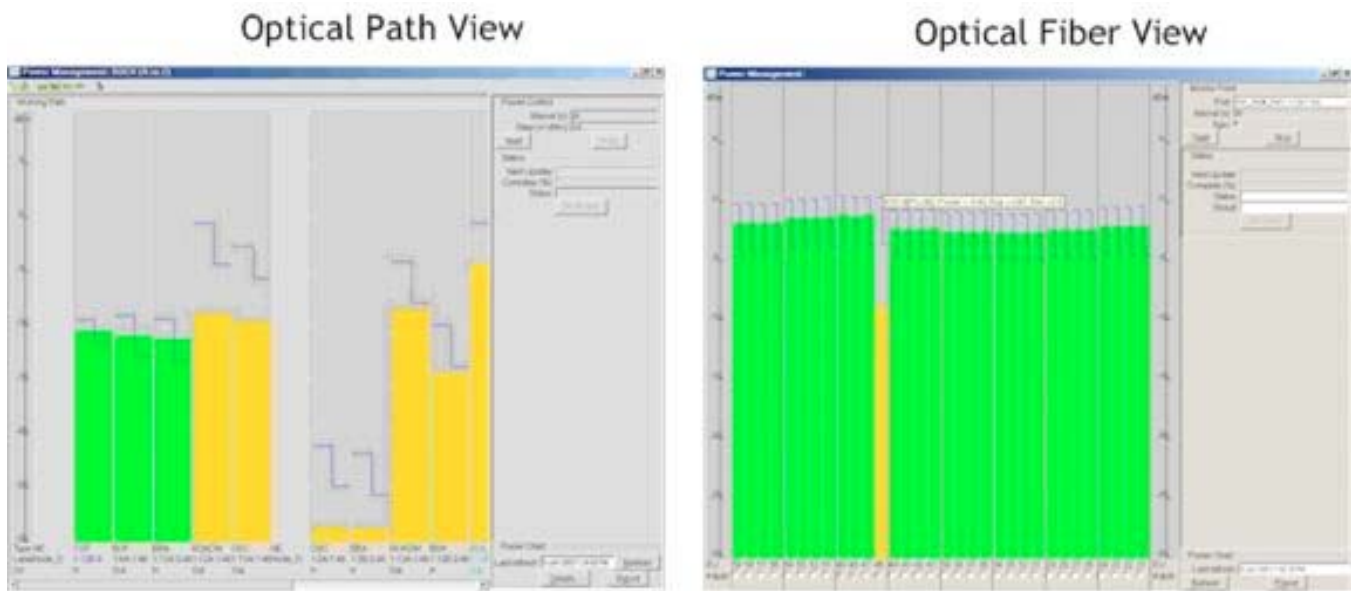
This is a process that operates continuously to keep optical levels at ideal set points and minimize optical power divergence throughout the life of the system. The result is zero-touch power management at node commission and when adding or removing wavelengths, and optimization of engineering rules.

Fault isolation

Whenever one or more optical powers fall outside their target zones, the occurrence is alarmed and provides a highly effective GUI that aids in troubleshooting. The data can be viewed in two different dimensions. One is the optical path view, which allows the operator to trace the power of a single wavelength from the point it enters the network until when it leaves. The other view is the optical fiber view, which shows the power of all wavelengths at a single point.

Refer to [Figure 14-25, “Wavelength tracker fault isolation”](#) (p. 14-74).

Figure 14-25 Wavelength tracker fault isolation



The first example shows the power trace of a wavelength through two nodes (horizontal scrolling allows viewing of the entire wavelength path), and the point in the first node where the power falls out of the target zone. The second example shows a point at which all but one of the wavelengths are within their target power range.

With this data, fiber bends, dirty connectors, incorrectly connected fibers, and so on, can be isolated to a specific node and also to particular interconnect points within that node.

This capability brings fault isolation out of the complex domain of analog optics with its expensive test equipment and highly skilled craft, and into the domain of SDH/SONET-like manageability.

APR support

APR is normally triggered by a combination of two triggers, OSC LOS and DWDM LOS. However, on spans that are pumped with a RAMAN amplifier, DWDM LOS becomes difficult to detect. due to amplified spontaneous emission (ASE) noise created by the RAMAN within the fiber span. The ASE propagates to the input detector of the ingress LD, and provides a high enough power reading to prevent DWDM LOS detection. Starting in Release 3.6.50, Wavelength Tracker tone detection is supported as a second trigger for APR, but only on Raman-pumped spans.

Keyed and unkeyed optical channels

The Alcatel-Lucent 1830 PSS supports both keyed and unkeyed optical channels. For keyed optical channels, Wavelength Tracker functionality is enabled. For unkeyed (unmanaged) optical channels, Wavelength Tracker functionality is not enabled. With unkeyed channels, encoders/fVOAs on OTs are not populated or enabled for integrated eVOAs, and decoder points are not used for monitoring or maintenance functions.

Note: All CWDM optical channels are unkeyed.

An NE can support both keyed and unkeyed optical channels.

The following external VOAs are supported on the pluggable OTs for keyed and unkeyed services.

For keyed services

- On the 11DPE12, 11DPE12A, 11DPE12E, 11DPM12, 11QPA4(A), 11QPE24, and 4DPA4 OTs, the VA port is equipped with an fVOA.
- On the MVAC, the G{1-8} port is equipped with an fVOA.

For unkeyed services

- On the 11DPE12, 11DPE12A, 11DPE12E, 11DPM12, 11QPA4(A), 11QPE24, and 11PPEN4 OTs, the VA port is optionally equipped with a sVOA. If a sVOA is not used, attenuators are installed in the transmission path for power control.
- On the 4DPA4, the VA port is not equipped. Attenuators are installed in the transmission path for power control. fVOAs and sVOAs are not supported for unkeyed services on the 4DPA4.
- On the 4DPA2, the VA port is not equipped. Attenuators are installed in the transmission path for power control; sVOAs and fVOAs are not supported. The 4DPA2 does not support keyed services.
- On the MVAC, the G{1-8} port is equipped with an sVOA or fVOA.

The table below summarizes the supported eVOAs per card type.

Table 14-7 DWDM OT VOA usage

Card	Service	fVOA	sVOA	No eVOA
11DPE12	Keyed	Y	—	—
	Unkeyed	—	Y	Y
11DPE12A	Keyed	Y	—	—
	Unkeyed	Y	Y	Y
11DPE12E	Keyed	Y	—	—
	Unkeyed	Y	Y	Y

Table 14-7 DWDM OT VOA usage (continued)

Card	Service	fVOA	sVOA	No eVOA
11DPM12	Keyed	Y	—	—
	Unkeyed	Y	Y	Y
11QPA4(A)	Keyed	Y	—	—
	Unkeyed	—	Y	Y
11QPE24	Keyed	Y	—	—
	Unkeyed	—	Y	Y
11QPEN4	Keyed	Y	—	—
	Unkeyed	—	Y	Y
4DPA2	Unkeyed	—	—	Y
4DPA4	Keyed	Y	—	—
	Unkeyed	—	—	Y
MVAC	Keyed	Y	—	—
	Unkeyed	Y	Y	—

Unmanaged (unkeyed) services

The Alcatel-Lucent 1830 PSS supports the addition of optical channel trails that are intentionally without wave keys. These trails are known as unkeyed Optical Channels (uOCh). Currently, configurations with unmanaged OCH services are intended for point-to-point end-terminal networks and linear chains with up to four nodes.

Unkeyed optical channel trails have the following characteristics:

- FOADM degrees using OSCT only support unkeyed cross-connects.
- No per-channel power monitoring is provided for these trails by a network element. Manual intervention may be required by field personnel with optical spectrum analyzing equipment to determine channel power.
- No per-channel trail identification is provided at the optical layer. The user must rely on a termination point trail trace identifier.
- Little or no fault localization is provided.
- No automated adjustment for per-channel power changes.
- Limited manual adjustments for per-channel power changes.
- Manual optical channel trail construction requires external test equipment and personnel at multiple sites.

Optical channel trails (the combination of termination transponders, optical spans and OCh cross-connects) are either managed or unkeyed for their entire length. An unkeyed optical channel cannot be provisioned with OPS protection. NE software will prevent this

configuration. The system will not allow unkeyed optical channels to be provisioned through an OPSA or WR card. Unkeyed Optical channels with WTOCM/WTOCMA are only supported on FOADM, ILA, and TOADM nodes with auto power management.

WTOCM/WTOCMA support for unkeyed services

WTOCM/WTOCMA provides unkeyed service support which includes features and support for optical nodes types and power management types that are not supported without it.

Support for unkeyed services with WTOCM/WTOCMA includes:

- Unkeyed optical channels mixed with keyed channels on auto power managed lines
- Unkeyed channels on WDM TOADM nodes
- Channel power information through WTOCM/WTOCMA monitoring for unkeyed channels
- Limited light-path tracing for unkeyed channels with WTOCM/WTOCMA monitoring.
- Alarms for Channel Missing and Channel power out of range on unkeyed channels at WTOCM/WTOCMA monitored ports

Support for unkeyed services without WTOCM/WTOCMA includes:

- Unkeyed channel provisioning
- Unkeyed channels on WDM FOADM and ILA lines
- Unkeyed channels on manually power managed FOADM and ILA lines

Table 14-8 Configurations with WTD or WTOCM(A)

Configuration	With WTD		With WTOCM(A)	
	Manual power management	Auto power management	Manual power management	Auto power management
FOADM	Yes	Yes ¹	Yes	Yes ¹
TOADM	No	No	Yes	Yes
ROADM	No	No	No	No
ILA	Yes	Yes ²	Yes	Yes
Anydirection	No	No	No	No

Notes:

1. If the FOADM node is an End-Terminal (1-degree), the system supports auto power management. If the FOADM node is 2-degrees or higher, the system will not support auto power management; the system must be manually power managed.
2. Supported, but only if **WtdPpcOffAlmOff**.

WTOCM/WTOCMA packs are required to monitor unkeyed channels for the following supported line types:

- Optical Add/Drop multiplexer nodes: TOADM or DFOADM lines.
- Dynamic gain equalizer (DGE) nodes: TOADM lines.

WTOCM/WTOCMA packs are optional for the following supported line types:

- In-line amplifier (ILA) nodes: ILA lines.

Alien wavelengths

Overview

The Alcatel-Lucent 1830 PSS-32 and Alcatel-Lucent 1830 PSS-16 accept “black and white” (B&W) client optical signals and convert them into ITU-T grid-compliant DWDM line signals, as is typical with all WDM systems. The line card that performs this function is the optical transponder. Among other functions, it performs O-E-O conversion and provides a manageable demarcation between the Alcatel-Lucent 1830 PSS (transport) and client switching equipment.

However, if the client equipment is capable of supporting native ITU-T grid-compliant DWDM interfaces, it may not be necessary to use an Alcatel-Lucent 1830 PSS optical transponder: the Alcatel-Lucent 1830 PSS can accept such “alien wavelengths” without any O-E-O conversion. Even in this case, there are many advantages to using optical transponders, but sometimes there is a prevailing advantage in the economics of alien wavelengths.

In some systems, alien wavelengths are directly launched into the DWDM filters. With no demarcation, this practice is fraught with operational problems.

Alcatel-Lucent 1830 PSS offers a mediating card creating a demarcation point between the client and DWDM system. The card establishes a monitoring point and has a VOA to control launch power. Uniquely, the card also has a WaveKey encoder that enables optical performance monitoring and wavelength tracing of the alien wavelength as it traverses the Alcatel-Lucent 1830 PSS domain—providing for unrivalled management of alien wavelengths.

The following cards support alien wavelengths:

- OPSA
- MVAC
- MVAC8B
- SVAC

Synchronization

Overview

Purpose

This section provides information the support of the Precision Time Protocol by Alcatel-Lucent 1830 PSS.

Contents

IEEE 1588v2 Precision Time Protocol (PTP)	14-81
---	-----------------------

IEEE 1588v2 Precision Time Protocol (PTP)

Overview

IEEE 1588 PTP is a message protocol similar to NTP, that operates closer to the physical layer. PTP can be used to distribute time of day, a common Epoch or Frequency. It maintains synchronization between master and slave clocks, but unlike standard NTP in the server, PTP distributes the time to slaves using multicast rather than by responding to requests from the slaves as with NTP.

IEEE 1588 PTP was originally developed for measurement and automation applications in a small geographic area. IEEE 1588v2 has revisions and its performance enhancements for use in Telecom network applications, where it can operate in a wider geographic area. Modifications in IEEE1588v2 include:

- Increased refresh interval increased from 1 per second to 128 Hz.
- Packet size has been reduced to reduce bandwidth usage and the ability to support additional distribution methods beyond multicast.
- Redundancy support (active/standby server support).

IEEE 1588 PTP clocks

The Precision Time Protocol uses a number of types of system clocks for synchronization of PTP across a network. They include:

- **Grandmaster Clock:** Within a domain, a clock that is the ultimate source of time for clock synchronization using PTP.
- **Ordinary Clock:** A clock that has a single Precision Time Protocol (PTP) port in a domain and maintains the timescale used in the domain. It may serve as the source of time, as a master clock, or may synchronize to another clock, as a slave clock.
- **Boundary Clock:** A clock that has multiple Precision Time Protocol (PTP) ports in a domain and maintains the timescale used in the domain. It may serve as the source of time, as a master clock, or may synchronize to another clock, as a slave clock.

The Boundary Clock was devised to support multiple PTP ports and a clock hierarchy which terminates the IEEE 1588 flow on one receiving link and then acts as a IEEE 1588 master for all outgoing links.

-
- **End-to-End Transparent Clock:** A transparent clock that supports the use of the end-to-end delay measurement mechanism between slave clocks and the master clock. An end-to-end transparent clock node will pass all PTP messages according to the addressing rules of the network, however those messages are modified to correct for the time spent traversing the node (the so called residence time). Thus, each node appears to be a "wire" which does not skew the time calculation for packets passing through it.
 - **Peer-to-Peer Transparent Clock:** A transparent clock that, in addition to providing Precision Time Protocol (PTP) event transit time information, also provides corrections for the propagation delay of the link connected to the port receiving the PTP event message. In the presence of peer-to-peer transparent clocks, delay measurements between slave clocks and the master clock are performed using the peer-to-peer delay measurement mechanism.

Standard Compliance

The IEEE 1588 features implemented on Alcatel-Lucent 1830 PSS are compliant with the ones specified in IEEE1588-2008, except for the following differences:

- In IEEE1588-2008, the PTP clock is either a One-Step clock or Two-Step clock. However, on Alcatel-Lucent 1830 PSS this attribute is defined for a PTP port other than for a PTP clock.

Feature capabilities

Alcatel-Lucent 1830 PSS supports PTP with the following capabilities:

- **Clock scope:** card-level PTP clock is supported
- **Clock mode:** Ordinary Clock (master or slave) and Boundary Clock are supported.
- **Clock type:** One-step clock is supported.
- **Delay measurement scheme:** The end-to-end delay measurement mechanism is supported.
- **PTP packet encapsulation:** PTP over Ethernet per Annex F of IEEE1588-2008 is supported.
- **BMC algorithm:** The IEEE1588-2008 default BMCA is supported.
- **IEEE 1588 messages:** Announce, Sync, Delay_Req, Delay_Resp messages are supported. IEEE 1588 management and signaling messages are dropped.
- **TLV:** TLV and Unicast negotiation are not supported.
- **ToD format:** The UBX/CM format is supported

IEEE 1588 PTP circuit packs

The following three types of cards support PTP on Alcatel-Lucent 1830 PSS:

- PTPCTL, which implements the physical layer clock (syncE) to distribute frequency and the PTP clock to distribute time/phase across the network.
- PTPIO, which provides adaptation for transport of PTP over WDM links.
- IEEE 1588-capable OTs: 11DPE12A (since Release 6.0), 11QCE12X and 11OPE8 (Hardware- ready)

In Release 6.0, the 11DPE12A supports IEEE 1588 PTP

IEEE 1588 PTP Architecture

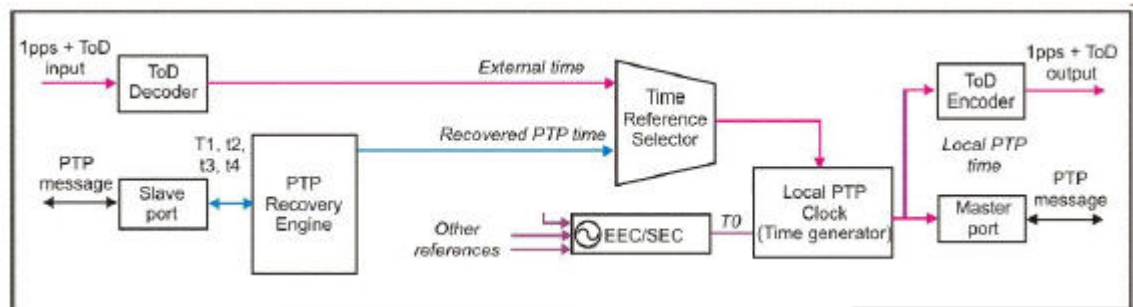
Alcatel-Lucent 1830 PSS supports the following clock types:

- Ordinary Clock (OC) – Master
- Ordinary Clock (OC) – Slave
- Boundary Clock (BC)

Alcatel-Lucent 1830 PSS supports distribution of the following timing characteristics through IEEE1588v2:

- Phase
- Time Of Day

Figure 14-26 Example system architecture supporting Ordinary Clock/Boundary Clock



The main functional blocks of such a PTP clock application are:

- ToD Decoder – This block retrieves the time of day from the external 1pps+ToD input interface.
- ToD Encoder – This block takes the local IEEE1588 time and converts it to the required ToD format for the external 1pps+ToD output interface.

- **Master Port(s)** – This block is responsible for distributing the IEEE1588 time of day over the packet network to the slaves. It generates PTP packets (Announce/Sync/Delay_Resp) toward the next slave in the time distribution chain and receives the PTP messages (Delay_Req) sent by its slave. An OC slave clock has no master port, while an OC master clock or BC may have multiple master ports.
- **Slave Port** – This block is in charge of communicating with its master through the PTP messages. It receives the PTP messages (Announce/Sync/Delay_Resp) from its master port and sends PTP messages (Delay_Req) to the master. An OC master clock has no slave port, an OC slave clock has one slave port, and a BC may have one slave port. Besides the master/slave ports, an OC/BC clock may also have PTP ports in the passives states.
- **PTP Recovery Engine** – This block is responsible for recovery of the PTP clock. It obtains the timestamps of t1, t2, t3 and t4 from the slave port. These timestamps are used to recover the frequency and time.
- **EEC/SEC** – This block selects the best frequency reference from the available clocks and provides it to the physical layer for frequency distribution. The selected reference also provides a stable frequency source for the local PTP clock. The function of this block is defined in G.8262 (EEC) and G.813 (SEC).
- **Local PTP Clock** – This block is responsible for generating the local IEEE1588 time. It uses a selected frequency reference to drive the time counter, and uses a selected time reference to bias or adjust the time counter.
- **Frequency reference selector** – This block selects the frequency reference for the local PTP clock. The reference frequency could come from the EEC/SEC or PEC.
- **Time reference selector** – This block selects the time reference for the local PTP clock. The time reference could come from the external 1pps+ToD input interface or the PTP recovery engine

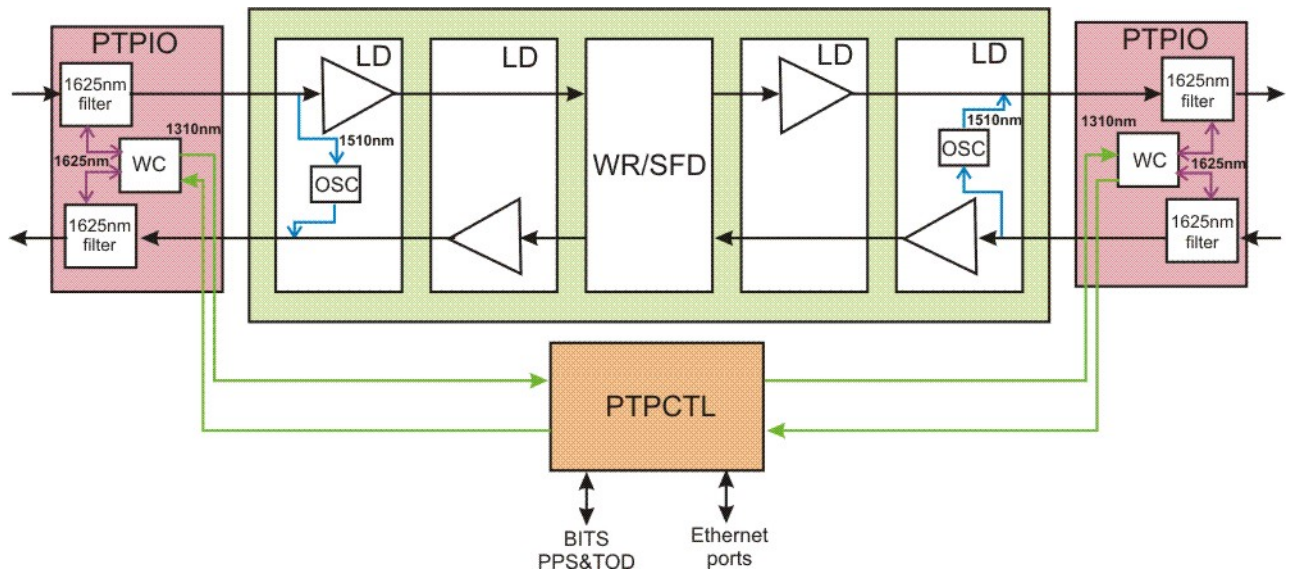
1588 PTP implementation

Alcatel-Lucent 1830 PSS currently supports a Card-level PTP system, containing a single IEEE 1588-capable OT card (11DPE12A) or a single PTPCTL card with PTPIO card, if the PTPIO is needed to support PTP transport over WDM links. All PTP ports and PTP control and management functional modules reside in the same card.

The following timing distribution scenarios are possible:

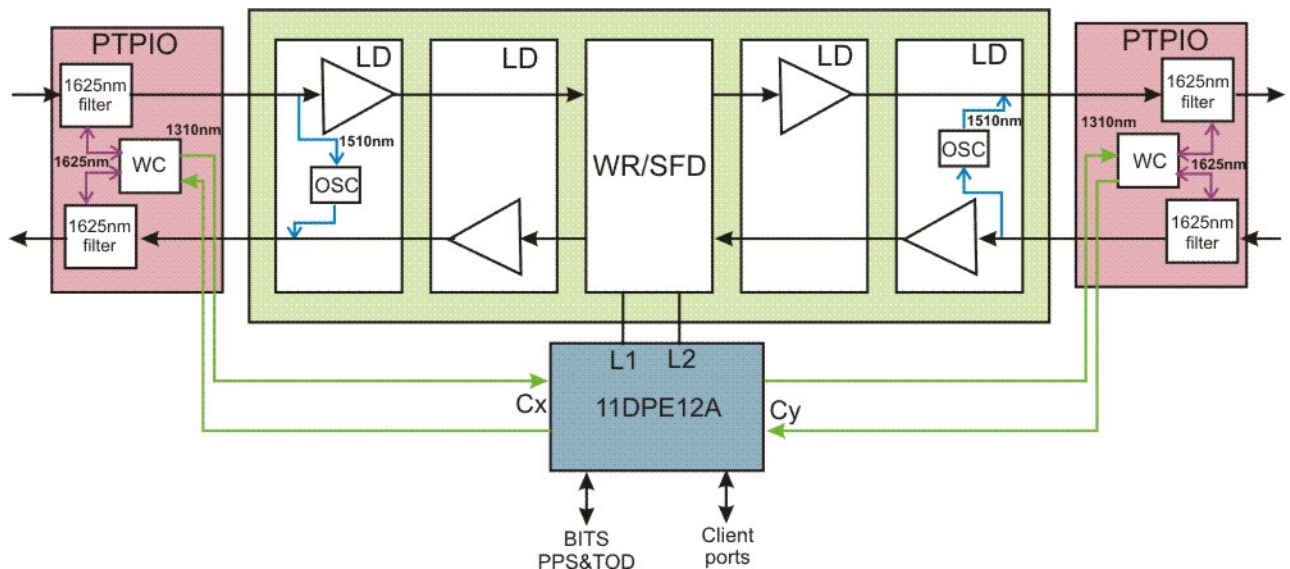
Card-level clock with PTPCTL + PTPIO

This scenario could be applied to WDM core nodes, including ILA, on Alcatel-Lucent 1830 PSS-4, PSS-16, or PSS-32 shelves. (See appropriate Alcatel-Lucent 1830 PSS-4, documentation for specifics of the PSS-4 shelf.)



Clock with 11DPE12A and PTPIO

This scenario could be applied to access ring nodes with 11DPE12A, on Alcatel-Lucent 1830 PSS-4, PSS-16, or PSS-32 shelves. The L1 clock of the 11DPE12A works in master mode. (See appropriate Alcatel-Lucent 1830 PSS-4, documentation for specifics of the PSS-4 shelf.)



Clock interconnection between PTPCTL cards

The PTPCTL cards in the same NE could be cascaded through the Ethernet ports to provide more ports connecting with other nodes. In this case, each PTPCTL card works as a standalone clock.

Clock interconnection between PTPCTL and 11DPE12A cards

The PTPCTL card and the 11DPE12A card could be cascaded through the Ethernet ports so that the timing information could be delivered from one card to the other. In this case, each PTPCTL/11DPE12A card works as a standalone clock. The connected Ethernet port is for timing distribution only.

IEEE 1588v2

IEEE 1588v2 is supported on the 11OPE8 and 11QCE12X cards.

Card-level PTP in 11OPE8 and 11QCE12X

The IEEE1588v2 subsystem on 11OPE8 and 11QCE12X supports the following:

- IEEE1588v2 based, Ordinary Clock (OC) Master/Slave or Boundary Clock (BC) functions
- Time/phase distribution over in-band channel in GbE (11QCE12X)/10GbE/ODU2e payload
- Support IEEE1588v2 default profile, and hardware ready for Telecom profile (G.8275.1)

These functions are limited to the distribution and recovery of time and phase. Frequency is distributed/recovered by the SyncE feature and is used by the PTP features (for example, timestamp counters).

Figure 14-27 11OPE8 PTP functionality

11OPE8 PTP Functionality Card Architecture and Faceplate

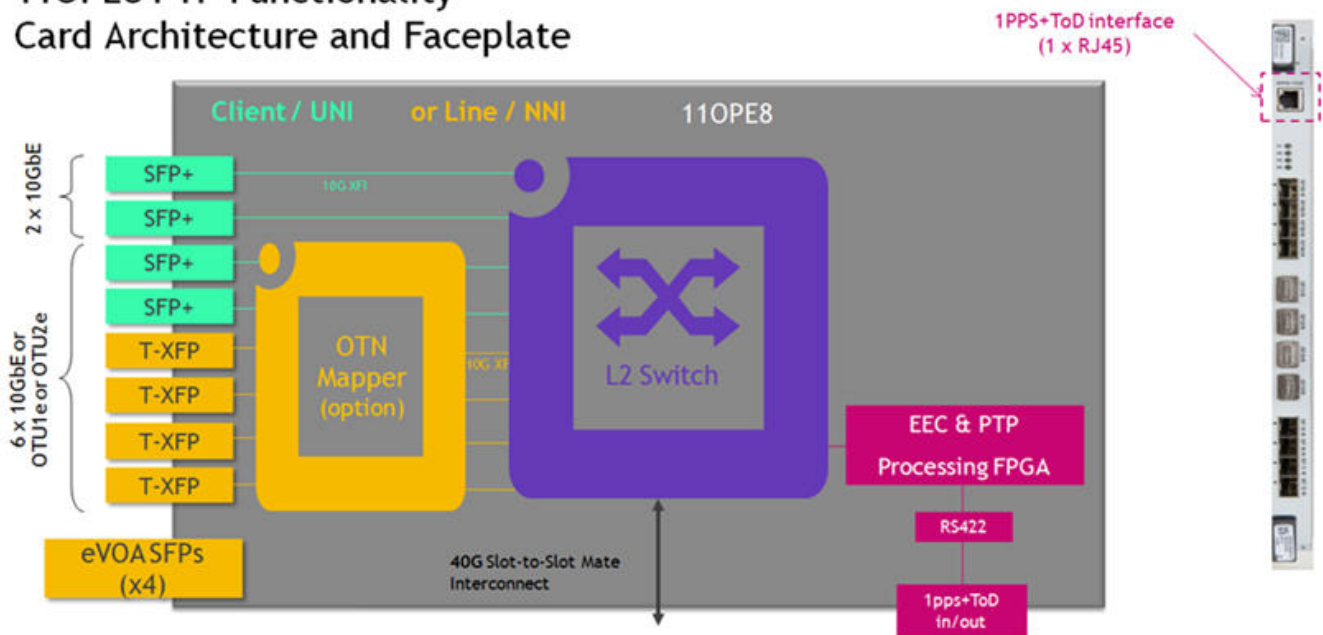
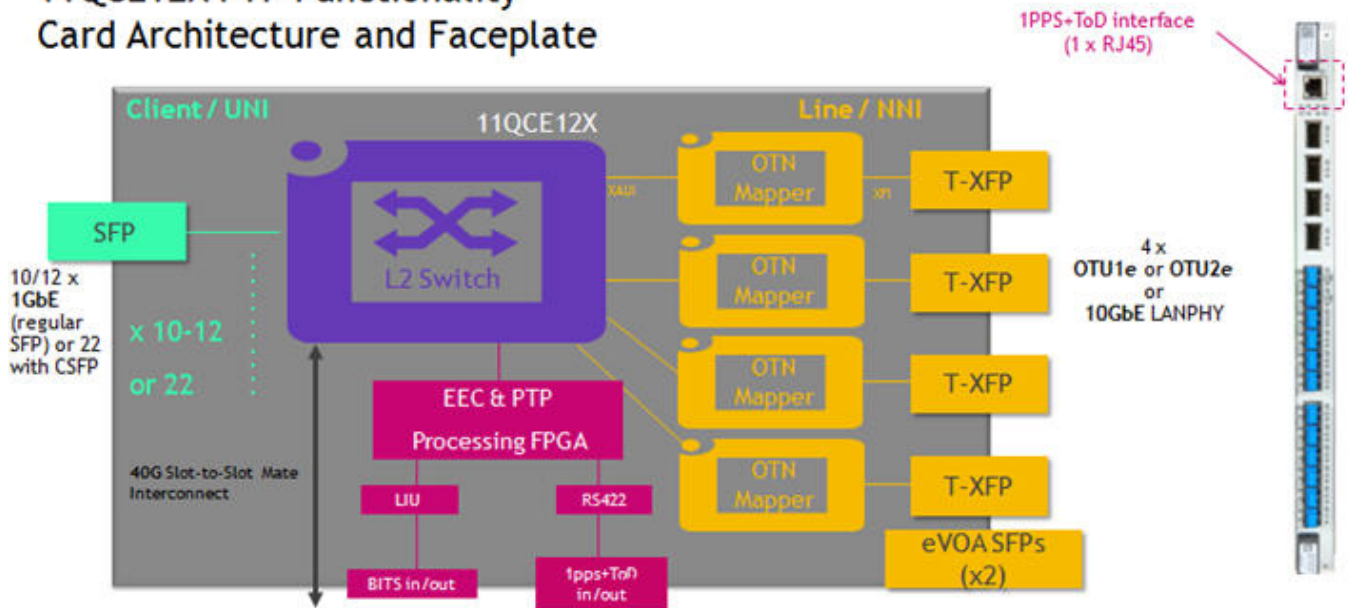


Figure 14-28 11QCE12X PTP functionality

11QCE12X PTP Functionality Card Architecture and Faceplate



External 1PPS&ToD interfaces

The 11OPE8/11QCE12X card provides one external 1PPS&ToD interface that can be configured as input or output and this interface uses an RJ45 connector.

On 11OPE8/11QCE12X, the 1PPS&ToD input interface is implemented as a PTP master clock, which sends the Announce/Sync messages to the local OC/BC every second.

When configured as output, the 1PPS&ToD interface indicates the time of the local PTP clock.

PTP ports

The PTP-capable ports receive PTP packets from the network and transmit PTP packets to the network.

11OPE8 supports different kinds of PTP ports:

- Client and Line interfaces: C1~C2, X1~X6, M1~M4

The 11OPE8 card provides 12 client and line 10GbE/OTU2e/OTU1e ports, each of which can be enabled or disabled for the PTP functionality independently.

11QCE12X supports different kinds of PTP ports:

- Client FE/GbE Interfaces: C1~C22

The 11QCE12X card provides 22 client FE/GbE ports, each of which can be enabled or disabled for the PTP functionality independently.

A PTP port is able to support transporting PTP packets over Ethernet as specified in IEEE1588-2008 Annex F.

- Line 10GbE/OTU2e/1e and mate-link Interfaces: X1~X4, M1~M4

When a line port of the 11QCE12X card is provisioned as a 10GbE interface, it can be enabled or disabled for the PTP functionality. A 10GbE port is able to support transporting PTP packets over Ethernet as specified in IEEE1588-2008 Annex F.

Note: All physical ports may be enabled for PTP independently.

OC/BC PTP engine

OC/BC PTP engine is active when 11OPE8 works as a standalone PTP clock and not in conjunction with PTPCTL card. It is responsible for terminating PTP1588 packets and recover/propagate time (1PPS/ToD).

PTP engine is active when 11QCE12X works as a standalone PTP clock. It is responsible to handle the IEEE1588v2 packets and to recover the time. These functions are implemented by the local OC/BC.

11OPE8/11QCE12X uses the four timestamps exchanged using the IEEE1588v2 messages to determine the offset between the 11OPE8/11QCE12X time base and the peer master clock time base. The 11OPE8/11QCE12X determines the offset adjustment and then in between these adjustments, 11OPE8/11QCE12X maintains the progression of time using the physical layer frequency assist.

Alcatel-Lucent 1830 PSS - Secure Data Center Connect (DCC) features

Overview

Purpose

This section provides information related to the Secure Data center connect features.

Contents

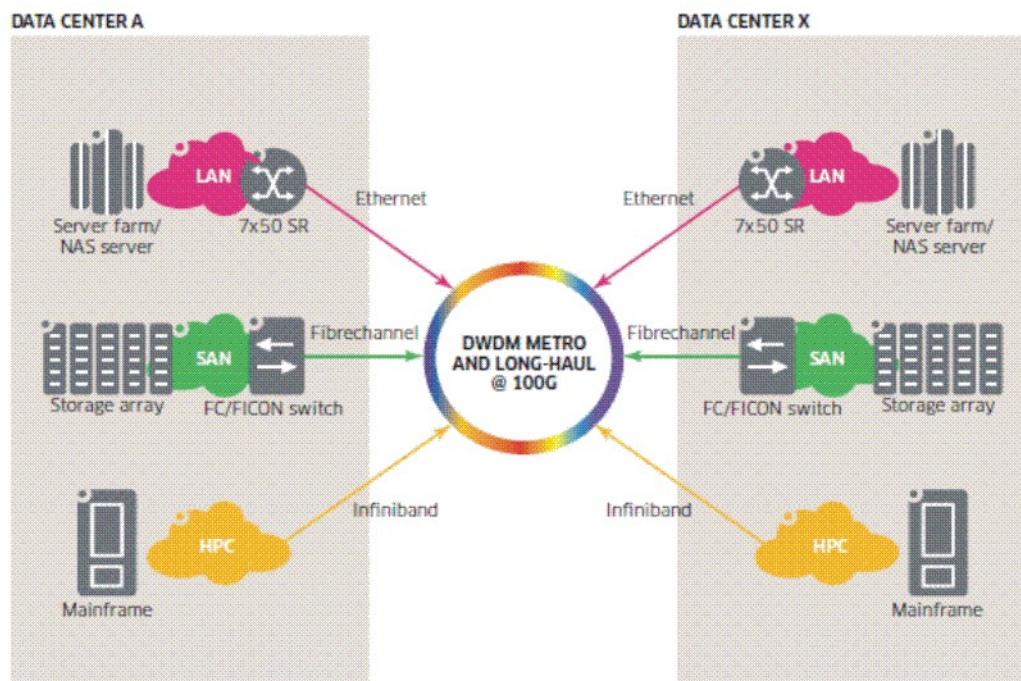
Data Center Connect	14-90
DWDM T-ROADM for DCC	14-95
Alcatel-Lucent 1830 PSS DCC features	14-96
Alcatel-Lucent 1830 PSS DCC security	14-98

Data Center Connect

Overview

The expansion of storage facilities, introduction of mission critical services, and new regulatory requirements create new demands and requirements that must be met by the networking infrastructure. Specifically, the need for disaster recovery/business continuity (DR/BC) attains much higher importance for enterprise customers.

Figure 14-29 Data Center Connect application



This requires that the networking infrastructure must provide fast, dependable, reliable and efficient transport between the data centers. Applications like synchronous mirroring/replication necessitate network deployments limited to simple point to point architectures, over synchronous distances (< 200 km), interconnecting primary and secondary data centers. The protocol of choice for these type of applications is Fibre channel, which has stringent requirements in terms of delay and does not tolerate loss. WDM is the ideal mode of transport for Fibre channel, due to its ability to transport without loss and with very high degree of availability. These applications also require very low latency, as well as high capacity to accommodate increased bandwidth for storage facilities.

Additional applications like replication on tertiary backup and “cloud” computing, require storage and collaboration over asynchronous distances (distances in excess of 200 km), where the latency is not such an important issue. The primary protocol for these

applications is Ethernet. Therefore networking equipment must provide efficient support for Ethernet. WDM is well suited for this kind of transport because it offers the lowest possible cost-per-bit transport, and provides long haul operation. These applications also require efficient packet optical integration as well as dynamic operation through ROADM and GMPLS control plane, in conjunction with a Service Router.

DWDM transport for DCC

DCC built on DWDM provides the ultimate solution for addressing concerns related to data center evolution. Wavelength routers, tunable optics, and colorless optical transponders support connectivity from and through the DWDM platform. Multi-degree, directionless Reconfigurable Optical Add-Drop Multiplexing (ROADM) configurations add the flexibility for connecting any wavelength to/from any direction across the optical infrastructure. GMPLS controls signaling and addresses the real-time, dynamic nature of connectivity between optical DWDM sites. This feature list can be further enhanced by with full Ethernet aggregation capabilities. Security is a critical element in DCC that must be supported by providing encryption capabilities for mission-critical traffic. Finally, DCC requires high channel capacity (> 80 wavelengths per fiber) and high speed (10G, 40G, and 100G channels) to meet expanding capacity requirements between data center sites on the mesh.

Dedicated, high-speed channels (wavelengths or sub-wavelengths) on DWDM spans deliver low latency connectivity, and because the optical network does not process the traffic, there is no contention on the DCC channels between sites, resulting in loss less transport. DWDM can provide the highest level of availability (a key attribute required from the cloud), and highest level of flexibility for DCC. Finally, DWDM supports the metro and long haul and WAN connectivity for DCC, over spans greater than 2000 km.

DWDM has the following advantages in DCC applications:

- Flexibility and adaptability at 100G+
- Quick service turn-up to meet dynamic bandwidth requirements
- Low, predictable latency
- Guaranteed QoS
- Transport-grade reliability with multiple options for < 50 msec restoration
- Photonics-level OAM
- Support for multi-services traffic
- Capable of converged aggregation for Ethernet and SAN (Fibre channel) traffic
- Loss-less transport
- Backup and security strategies for redundancy often drive the geographical dispersions of DCs that can only be met by DWDM

DCC interfaces

The Alcatel-Lucent 1830 PSS supports the following interface types for DCC applications:

- Fast Ethernet, Gigabit Ethernet, 10 GE (LAN and WAN), and 100 GE
- 4x10GE Muxponder (40G) and 10x10 GE Muxponder (100G)
- Fibre channel 1G, 2G, 4G, 8G, and 10G
- FICON 1G, and 2G; and FICON-Express
- BM Intersystem channel ISC-3 peer-mode
- Video: SD-SDI, HD-SDI, DVB-ASI
- Transponderless (direct connection) support of ITU-grid wavelengths from external equipment

Muxponder and transport support

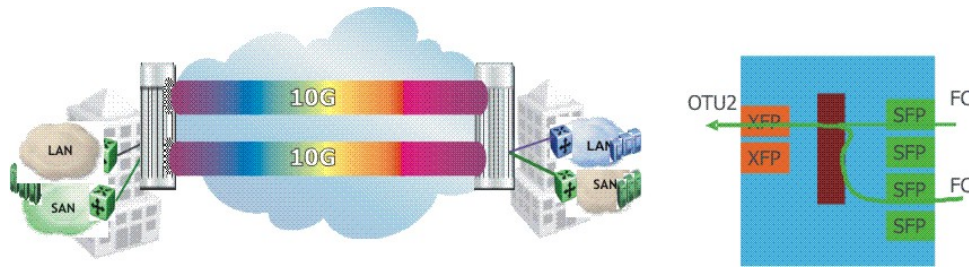
Alcatel-Lucent 1830 PSS provides several Muxponder and Transponder capabilities that allow for efficient Data Center Connect. These capabilities include support for Fibre channel and Ethernet clients, and are designed to provide comprehensive support for both applications over synchronous distances (private clouds), and asynchronous distances (public clouds).

Several packs support Fibre channel clients:

- Muxponder capability to mux FC 100; FC 200; FC 400 clients into a 10G OTU2 line (11STMM10, 11DPM12)
- Transponder capability to place FC 800 into a 10G OTU2 line and FC1200 clients into a OTU1f line (11QPA4)
- Encrypted Transponder capability to encrypt FC 800 into a 10G OTU2 line and FC 1200 clients into a 10G OTU1f line (11QPEN4)

In these 1830 PSS packs, multiple ingress Fibre channel client signals are muxed, or encapsulated, into an OTU2 line. The WDM system transports the composite signal to the its point of egress, where it is demuxed by the 1830 PSS pack, and signals are delivered to the client ports. In this type of application a point-to-point system is customary, to guarantee low latency. Distance is typically restricted by a 5 ms round trip time, necessitated by the applications, as well as the distance extensions from the Fibre channel switch. The role of WDM transport is to provide very low latency (typically ~20 microseconds per pack) and very high availability with full sub-50 ms protection.

Figure 14-30 Fibre Channel through OTU2 for DCC

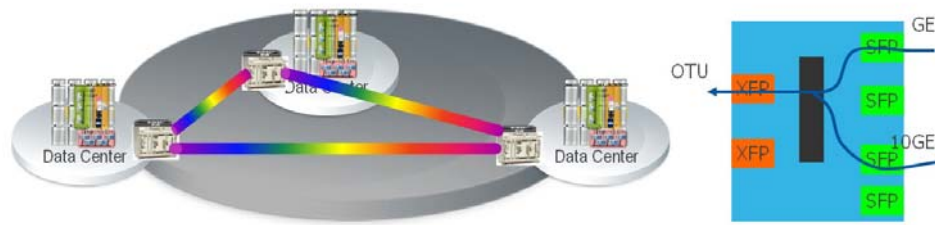


There are several packs that support Ethernet clients:

- Muxponder capability to mux 1GE clients into a 10G OTU2 line (11STMM10, 11DPM12)
- Muxponder capability to mux 10GE clients into a 100G OTU4 coherent (112SCX10, 112SNX10, 130SCX10, 130SNX10)
- Aggregation capability to aggregate 1GE clients, using statistical multiplexing, into a 10G OTU2 line (11DPE12, 11DPE12E)
- Transponder capability to put 10GE clients into a 10G OTU2 line (11QPA4)
- Muxponder capability to put 10GE clients into a 100G OTU4 line (112SDX11)
- Encrypted Transponder capability to encrypt 10GE clients, into a 10G OTU2 line (11QPEN4)

In these packs, many Ethernet client signals enter the pack and are muxed into an OTU2 or OTU3 line. Muxing can be either passive, or in some cards there is the capability to perform packet operation with statistical multiplexing, to better utilize the available bandwidth. The WDM system transports the composite signal to the 1830 PSS pack that is its point of egress.

Ethernet clients can be associated with applications that run over asynchronous distances (<1000 kms) where latency is not a critical factor. Hence, the networking topologies for such applications can be meshed, involving many hops and distances of up to 1000 kms. Ethernet clients are not restricted in terms of distance, since they are usually buffered which incurs latency, and a mechanism is provided to deal with packet loss. Therefore, a typical Ethernet signal may traverse multiple components, such as an Ethernet switch in the Data center, a service router, WDM equipment, and more. The significance of Ethernet applications is that they provide the foundation for cloud services, and are expected to grow rapidly.



It should be noted that many packs can support both Ethernet and Fibre channel clients.

Note: Packs supporting FC client signals have been qualified by EMC eLAB Testing and Brocade Fabric Aware Testing. Alcatel-Lucent 1830 PSS has been extensively tested with various FC/FICON switches used with storage equipment.

DWDM T-ROADM for DCC

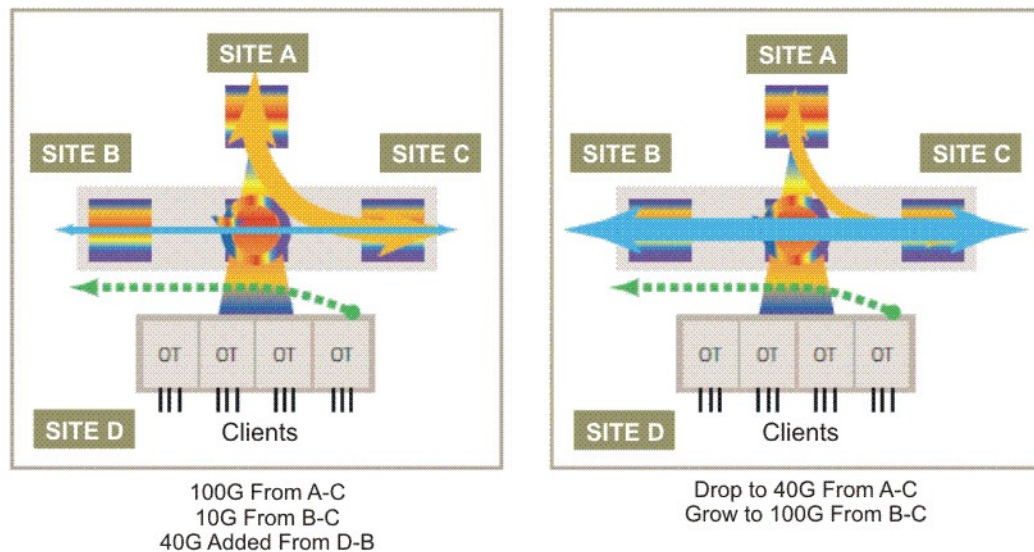
Overview

DWDM Tunable-Reconfigurable Optical Add-Drop Multiplexing (T-ROADM) configurations provide the highest level of scale and flexibility for switching data center traffic. They also support metro and long-haul reach, high reliability, and OA&M functions. DWDM delivers low latency across a predictable infrastructure of high-speed optical channels from 10G to 100G and beyond, and provides the lowest overall total cost of any DCC solution.

T-ROADM DCC support

T-ROADM supports rapid set-up and changes to wavelength transport across the entire DWDM network, as shown in [Figure 14-31, “Adding and dropping wavelengths for DCC” \(p. 14-95\)](#). This is required to support the dynamic nature of application and content traffic generated by enterprises into data centers, and between data centers. Combining many wavelengths onto a single fiber maximizes the efficiency of each fiber pair. Also, converging traffic types (Ethernet, FC, and IB) onto a single wavelength further increases the efficiency of each wavelength, maximizing overall utilization of the WAN. For fully converged DCC operation, packet aggregation functionality must be integrated into the ROADM, including support for the full set of Ethernet protocols.

Figure 14-31 Adding and dropping wavelengths for DCC



Alcatel-Lucent 1830 PSS DCC features

Overview

Alcatel-Lucent 1830 Photonic Service Switch (PSS) is a best-in-class DWDM platform, providing 100G coherent optics, T-ROADM, photonic OA&M, and metro to long-haul reach. It can scale from higher than 2 TB in a single chassis, to as low as a single slot shelf. The 1830 PSS also supports interchangeable line cards. This fourth generation Wave Division Multiplexing (WDM) solution was developed to maximize wavelength utilization levels, while meeting strict service level agreements (SLAs) with ultra-fast restoration and coordinated network management.

Alcatel-Lucent 1830 PSS provides scalable DWDM that supports data center aggregation of Ethernet and Fiber Channel (FC) data sources. Using internally developed silicon, the 1830 PSS was the first platform to support 100G coherent DWDM in a single wavelength. The 1830 PSS also supports efficient wavelength switching between source and destination using Tunable-Reconfigurable Optical Add-Drop Multiplexing (T-ROADM).

Key Features

Alcatel-Lucent 1830 PSS provides the following features in support of DCC applications:

- Support for L1 encryption at ultra-low latency
- Integrated intrusion detection with a 0.5 dB threshold, for immediate detection of potential interference on optical fibers
- Encryption key management, with hitless key rotation
- Certified interoperability with leading SAN switching and storage vendors (EMC, Brocade)
- Ethernet aggregation function, including support for Ethernet protocols
- Tunable and reconfigurable Optical Add-Drop Multiplexer (OADM) with single wavelength add-drop granularity
- Colorless and directionless add-drop of wavelengths up to 10 degrees
- Up to 88 wavelengths per fiber pair, using ITU 50 GHz grids, at 100G
- OTH G.709 transport interfaces at ODU1 (2.5G), ODU2 (10G), ODU3 (40G), and ODU4 (100G) rates, including integrated checksums to guarantee data validity
- Mix of 10G, 40G, and 100G DWDM onto a fiber pair
- 96x10G per rack and 15x100G interfaces per rack
- Optical reach of 1600 km @ 100G for 88 channels = 8.8 Tb/s of traffic per fiber
- Optical reach of 3200 km @ 10G or 40G for 88 channels
- Leading DP-QPSK coherent 100G optics, and DP-BPSK 40G coherent optics, without interference to existing 10G channels on a fiber pair

- Alien wavelength management
- Flexible protection/restoration options per wavelength, including diverse routed protection, dedicated and shared protection options, and 1+1 protection
- GMPLS/ASON cross-layer automation and resilience
- Wavelength Tracker (WT) to automatically monitor and adjust wavelengths and power levels at any point in the network, without requiring manual Optical Spectrum Analyzers (OSA)

Alcatel-Lucent 1830 PSS DCC security

Overview

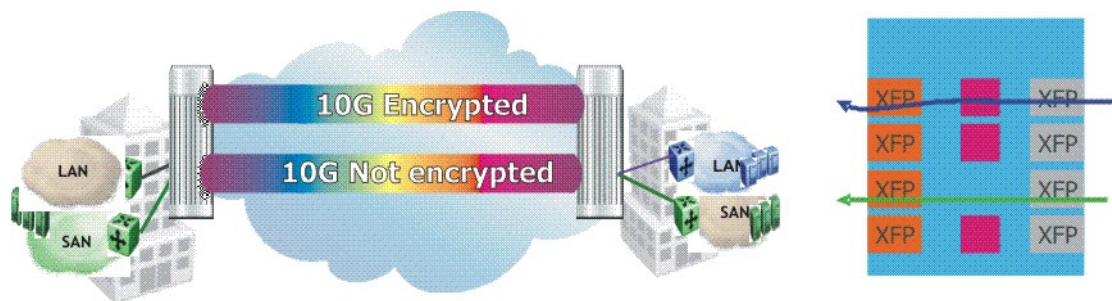
DCC transport risks are related to the uncertainty that vulnerabilities could be exploited to damage or remove sensitive data assets. Alcatel-Lucent 1830 PSS provides a comprehensive security solution aimed at customers with tier 1 applications, where security is of utmost importance. These usually include DR/BC applications of very sensitive information such as government, health, financial institutions etc.

Alcatel-Lucent 1830 PSS security solutions has the following important elements:

- Encryption function capable on encrypting 10G signals in L1, and featuring very low latency
- Key Management Capability
- Optical intrusion detection
- Secure mode of operation

Encryption capability

The first element of the solution is an encryption capability that is selectable per port, based on the standard AES256 Counter Mode algorithm as specified by National Institute of Standards, and incorporating block cipher to perform symmetric L1 encryption. This capability is provided by the 11QPEN4 pack which can directly encrypt 10GE, FC 800 and FC 1200 client signals at L1, append them with an OTU2 header, and sent them on to the line port. This provides encryption independent of the higher-layer protocol at bulk rates and with very low latency (<15 microseconds) that is suitable for the DCC applications.



Key management

The second element of the security solution is the Key Management Tool (KMT) that provides for management of the Keys used for the encryption. The KMT allows for separation of the network administrator and the cryptographic officer roles, and enables the cryptographic officer to assign and rotate the keys. KMT allows the end user to manage their own keys, independent of the provider, which allows complete security for customers.

Optical intrusion detection

The third element of the solution is Optical Intrusion Detection. It relies on periodic measurements of the power on the line and issues an alarm if power levels in consecutive measurements are below a specified value. A threshold value (from 1.0 dB to 3.0 dB, with steps of 0.5 dB) can be set to raise an alarm for possible optical intrusion when optical loss changes beyond the configured level.

Secure mode of operation

The fourth element is the “hardened” (secure) mode of operation. When in this mode, only the essential logical and physical ports needed to manage the system are open, only secure Network Management protocols are supported (SSL, SNMPv3), software debug functions are disabled, and services of the embedded OS are disabled, as well as any interactive OS access.

15 WDM Carrier Ethernet and MPLS-TP

Overview

Purpose

This chapter provides description to the Ethernet services and applications supported on 1830 PSS. Carrier Ethernet consists of technologies and protocols added to basic Ethernet to enable carriers to create Ethernet transport services that are reliable, maintainable, and able to meet service level agreements with their customers.

Contents

Ethernet OAM terminologies	15-2
Basic Ethernet services and features	15-6
Multiprotocol Label Switching - Transport Profile (MPLS-TP)	15-70
Ethernet OAM	15-82
Synchronous Ethernet	15-86
Smart device OAM demarcation and management	15-92

Ethernet OAM terminologies

Terminologies

The following section describes the common Ethernet OAM terminologies.

OAM transparency

OAM Transparency refers to the ability to allow transparent carrying of OAMPDU frames belonging to higher level MEGs across other lower level MEGs when the MEGs are nested. OAMPDU frames belonging to an administrative domain originate and terminate in MEPs present at the boundary of that administrative domain. A MEP prevents OAMPDU frames corresponding to a MEG in the administrative domain, from leaking outside that administrative domain. However, when a MEP is not present or is faulty, the associated OAMPDU frames could leave the administrative domain.

Similarly, a MEP present at the boundary of an administrative domain protects the administrative domain from OAMPDU frames belonging to other administrative domains. The MEP allows OAMPDU frames from outside administrative domains belonging to higher level MEs to pass transparently; while it blocks OAMPDU frames from outside administrative domains belonging to same or lower level MEs.

Proactive OAM

Proactive OAM refers to OAM actions which are carried out continuously to permit proactive reporting of fault and/or performance results.

On-demand OAM

On-demand OAM refers to OAM actions which are initiated through manual intervention for a limited time to carry out diagnostics. On-demand OAM can result in singular or periodic OAM actions during the diagnostics time interval.

Maintenance Entity (ME)

ME represents an entity that requires management and is a relationship between two Maintenance Entity Group End Points.

Maintenance Entity Group (MEG)

ME Group (MEG) includes different MEs that satisfy the following conditions:

- MEs in a MEG exist in the same administrative boundary
- MEs in a MEG have the same MEG Level
- MEs in a MEG belong to the same point-to-point ETH connection or multipoint ETH connectivity

Maintenance domain (MD)

The network or the part of the network for which faults in connectivity are to be managed.

Maintenance association (MA)

Maintenance Association includes different MEs that satisfy the following conditions:

- MEs in an MA exist in the same administrative boundary
- MEs in an MA have the same MD level
- MEs in an MA belong to the same VLAN

Maintenance Association Identifier (MAID)

An identifier for a Maintenance Association, unique over the domain that CFM is to protect. The MAID has two parts: the Maintenance Domain Name and the Short MA Name.

Maintenance End Point (MEP)

Maintenance End Point (MEP) is an end point of an MA which is capable of initiating and terminating OAM frames for fault management and performance monitoring.

Maintenance Intermediate Point (MIP)

Maintenance Intermediate Point (MIP) is an intermediate point in an MA which is capable of reacting to some OAMPDU frames (but not Y.1731). A MIP does not initiate OAMPDU frames.

It consists of two half-functions (MHF), one for each direction (see Up/Down-MP).

Server MEP

Y.1731 defines a server MEP as an abstraction for detecting faults at the physical layer to notify Ethernet MEP's. G.8021 does not use the concept and simply uHLI CI_SSF to include the physical layer fault in the equation for aAIS.

MD Level

In case MA's are nested, the OAM flow of each MA has to be clearly identifiable and separable from the OAM flows of the other MA's. In caHLI the OAM flows are not distinguishable by the ETH layer encapsulation itself, the MD Level in the OAMPDU frame distinguishes between the OAM flows of nested MAs.

Eight MD Levels are available to accommodate different network deployment scenarios.

Maintenance Domain

The network or the part of the network for which faults in connectivity are to be managed.

Down-MP

A MEP or an MHF residing in a Bridge that receives OAM PDUs from, and transmits them towards, the direction of the LAN.

Up-MEP

A MEP or an MHF residing in a Bridge that transmits OAM PDUs towards, and receives them from, the direction of the Bridge Relay Entity.

Primary VID

The VID, among a list of VIDs, on which all OAMPDU generated by MPs except for forwarded LTMs are to be transmitted.

Linktrace Message (LTM)

A multicast OAMPDU frame initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating a Linktrace Reply, up to the point at which the Linktrace Message reaches its destination or can no longer be forwarded.

Linktrace Reply (LTR)

A unicast OAMPDU frame sent by a Maintenance association Intermediate Point or Maintenance association End Point in response to receiving a Linktrace Message.

Loopback Message (LBM)

A unicast OAMPDU transmitted by a MEP, addressed to a specific MEP or MIP, in the expectation of receiving an LBR.

Loopback Reply (LBR)

A unicast OAMPDU transmitted by a MEP or MIP to a MEP, in response to an LBM received from that MEP.

Continuity Check Message (CCM)

A multicast CFM PDU transmitted periodically by a MEP in order to assure the continuity over the MA to which the transmitting MEP belongs. No reply is sent by any MP in response to receiving a CCM

Ethernet Alarm Indication Signal (AIS)

Ethernet Alarm Indication Signal function (ETH-AIS) is used to suppress alarms following detection of defect conditions at the server (sub) layer.

Ethernet Client Signal Fail (ETH-CSF)

Ethernet Client Signal Fail function (ETH-CSF) is used for a MEP to propagate to a peer MEP the detection of a failure or defect event in an Ethernet client signal when the client itself does not support appropriate fault or defect detection or propagation mechanisms, such as ETH-CC or ETH-AIS.

Ethernet Remote Defect Indication (RDI)

Ethernet Remote Defect Indication function (ETH-RDI) can be used by a MEP to communicate to its peer MEPs that a defect condition has been encountered. ETH-RDI is used only when ETH-CC transmission is enabled.

Ethernet Loss Measurement (ETH-LM)

ETH-LM is used to collect counter values applicable for ingress and egress service frames where the counters maintain a count of transmitted and received data frames between a pair of MEPs.

Ethernet Delay Measurement (ETH-DM)

ETH-DM can be used for on-demand OAM to measure frame delay and frame delay variation. Frame delay and frame delay variation measurements are performed by sending periodic frames with ETH-DM information to the peer MEP and receiving frames with ETH-DM information from the peer MEP during the diagnostic interval. Each MEP may perform frame delay and frame delay variation measurement.

Basic Ethernet services and features

Overview

The 1830 PSS supports several muxponders (combined multiplexer and transponder) with layer 2 packet switching capabilities. The 11STGE12, 11DPE12, 11DPE12E, 11DPE12A support Ethernet Virtual Private Line services. See [“Basic Ethernet services and features” \(p. 15-7\)](#)

- Ethernet Private Line (EPL) - An Ethernet service consisting of a single Ethernet VC (EVC) between two customer sites. For more information, see [“EPL and EVPL services” \(p. 15-7\)](#).
- Ethernet Virtual Private Line (EVPL) - An Ethernet service consisting of multiple EVCs between two customer sites. For more information, see [“EPL and EVPL services” \(p. 15-7\)](#).

The SROS L2 packet cards (11QPE24, 11QCE12X, and 11OPE8) support the full set of MEF Carrier Ethernet 2.0 services. The features described in this section below apply to all of the SROS L2 packet cards; exceptions are explicitly noted. Refer to [“Ethernet services and features on SROS L2 packet cards” \(p. 15-7\)](#)

- Ethernet LAN (E-LAN) - An Ethernet service that consists of multiple EVCs between multiple customer sites. For more information, see [“Ethernet LAN Service” \(p. 15-9\)](#)
- [“L2 Smart SFP & Smart cEDD remote management ” \(p. 15-48\)](#)
- [“MEF E-Tree service” \(p. 15-12\)](#)
- [“MEF CE-VLAN bundling \(VLAN range SAP\)” \(p. 15-16\)](#)
- Ethernet protection features:
 - [“ERP on 1G UNI & NNI and 10G UNI ports” \(p. 15-19\)](#)
 - [“ERP Ring Interconnection with DNI using Sub-Rings” \(p. 15-20\)](#)
 - [“Multi-Chassis LAG \(MC-LAG\) ” \(p. 15-42\)](#)

QoS features:

- [“IPv6 TC/DSCP ingress classification” \(p. 15-51\)](#)
- [“Color-aware policing \(E-NNI\)” \(p. 15-51\)](#)
- [“Weighted Random Early Detection \(WRED\) ” \(p. 15-51\)](#)
- [“QoS L3/L4 classification” \(p. 15-49\)](#)

Ethernet OAM and PM features:

- [“ITU-T Y.1731 LM/SLM and DM pro-active” \(p. 15-56\)](#)
- [“ITU-T G.7710 PM with 15/24 hrs binning and thresholding” \(p. 15-59\)](#)
- [“100ms period for ITU-T Y.1731 pro-active SLM and FLR accuracy improvement” \(p. 15-60\)](#)
- [“ETH-DM frame size configuration” \(p. 15-60\)](#)

- “SAP Ingress Meter/FC counters” (p. 15-64)
- “Egress queues counters” (p. 15-65)

Basic Ethernet services and features

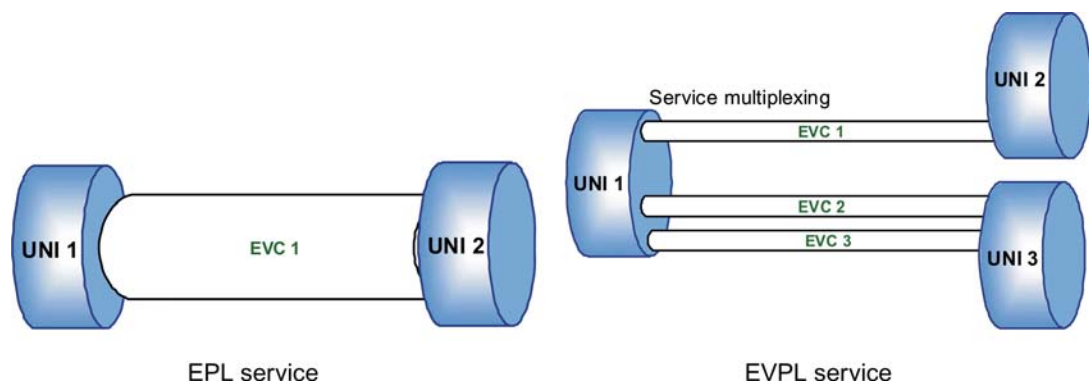
EPL and EVPL services

EPL service is the most popular service provided by the transport network due to its simplicity. With EPL, each Ethernet port can only contain a single Ethernet Virtual Connection (EVC). This type of service interconnects two Ethernet interfaces and generally provides fully transparent transport of customer frames.

EVPL service allows multiple EVCs within each Ethernet port. With EVPL, multiple Ethernet services can be multiplexed to a single port. VLAN IDs are generally used to distinguish between different services within the same port.

In 1830 PSS, the 11DPE12(E/A), 11STGE12, and SROS L2 packet cards support both the standard EPL and EVPL services, as illustrated in [Figure 15-1, “EPL and EVPL services”](#) (p. 15-7).

Figure 15-1 EPL and EVPL services



Ethernet services and features on SROS L2 packet cards

This section describes the services and features of the SROS L2 packet cards, namely the 11QPE24, 11QCE12X, and 11OPE8. Except where noted otherwise, all of these features apply to all of the SROS L2 packet cards.

Ethernet features

L2CP processing compliant to MEF 6.1.1 EPL Option 2 on SROS L2 packet cards

A Layer 2 Control Protocol Service (L2CP) Frame is a service frame whose destination MAC address lies in the range [01-80-C2-00-00-00 through 01-80-C2-00-00-0F] (Bridge Block of protocols) and [01-80-C2-00-00-20 through 01-80-C2-00-00-2F] (GARP Block of protocols). It can be untagged or tagged but is normally untagged on a UNI. Any such frame MUST be treated as a L2CP frame according MEF requirements in MEF 6.1.1.

In R8.2, EPL Option 2 is supported.

EPL Option 2: *Circuit-like EPL* with maximum level of transparency (tunnel everything except Pause) - intended to mimic TDM Private Line services and legacy Ethernet over SDH/SONET services Optional in MEF.

The treatment of Service frames with other MAC DAs is outside the scope of MEF recommendations but a service provider may define additional addresses for identifying L2CP.

In R8.2, the enhancement is to add tunneling for IEEE 802.1AB LLDP and IEEE 802.1X PAE PDUs. This is done through new CLI commands and complies with the EPL Option 2 defined in MEF 6.1.1 and MEF 45.

The SROS L2 packet cards support the following Carrier Ethernet features:

- Supports L2CP processing compliant to MEF 6.1.1 EPL Option 2:
 - Supports implementing provisionable option to comply with EPL Option 2 for more transparency and is supported in PSS-8, PSS-16, PSS-16II and PSS-32 shelves
 - Provides an option to tunnel the following L2CP:
 - IEEE 802.1AX port authentication
 - IEEE 802.1AD LLDP
 - Supports the following SAPs:
 - Dot1q explicit NULL SAP (:0 SAP) and Dot1q default SAP (:* SAP)
 - And NULL SAP

Note: It is recommended to use this feature only when a VPLS is used to emulate a point to point service (that is, an EVPL/EPL configured using a 3-point VPLS Service, with one access SAP and 2 access-uplink SAP for redundant connectivity). If the VPLS service is used for multipoint connectivity, it is not recommended to use this feature. When a layer-2 control frame is forwarded out of dot1q SAP or a QinQ SAP, the SAP tags of the egress SAP are added to the packet.

Per-slot upgrade for SROS L2 packet cards

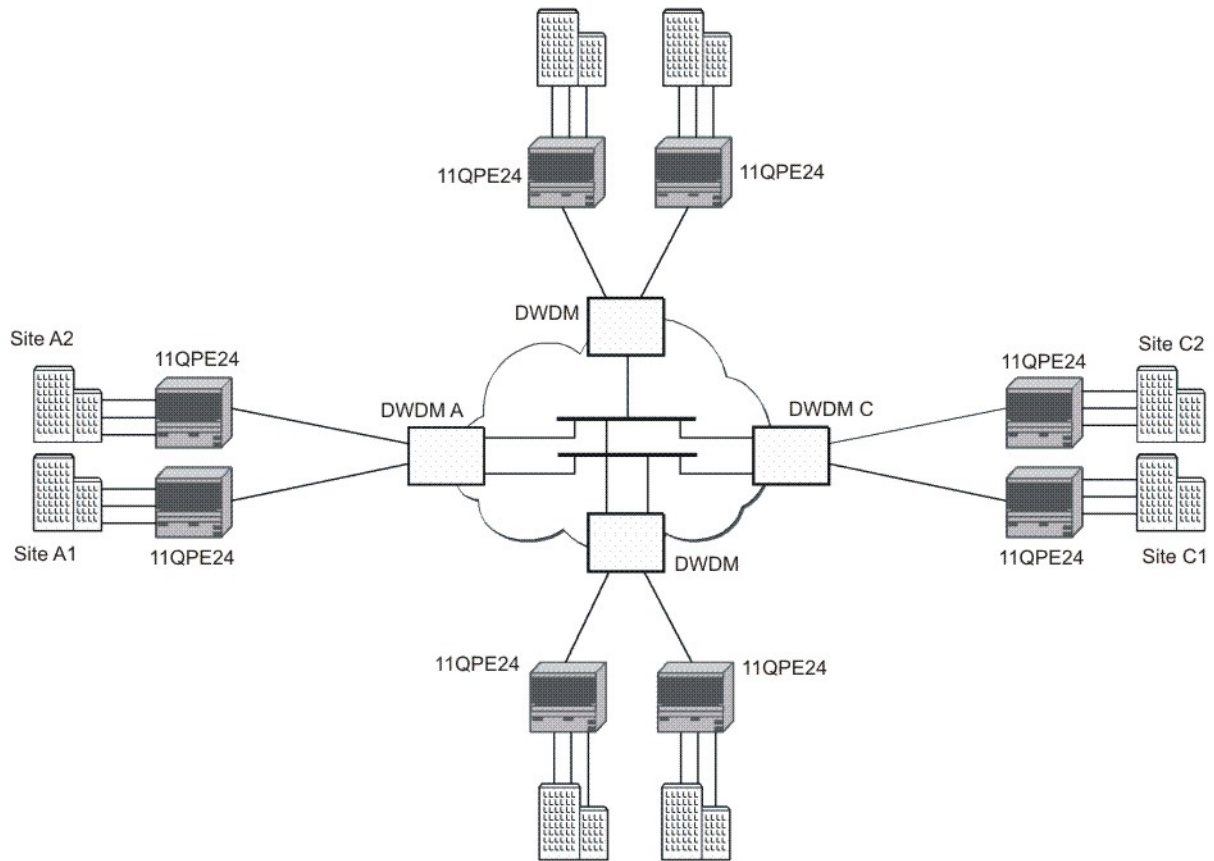
The SROS L2 packet cards do not support hitless upgrade, so they are always skipped by NE during in-service upgrade (ISUG) process. The user needs to upgrade/warm-reboot the cards through manual procedures after the NE ISUG. The upgrade of each card is performed under user control at a convenient time in order to reduce the impact of the traffic outage. Traffic interruption during a software upgrade can be minimized by using ERP and MC-LAG with a pair of cards and upgrading the cards of the pair sequentially.

Ethernet LAN Service

Ethernet LAN Service (E-LAN) is a class of virtual private network service that allows the connection of multiple sites in a single bridged domain over a provider-bridge Q-in-Q network. It can also be private, similar to E-Line: EP-LAN or EVP-LAN. The customer sites in an E-LAN instance appear to be on the same LAN, regardless of their location. E-LAN uses an Ethernet interface on the customer-facing (access) side which simplifies the LAN/WAN boundary and allows for rapid and flexible service provisioning.

An E-LAN service provides connectivity between two or more SAPs. The connection appears to be a bridged domain to the customer sites so protocols, including routing protocols, can traverse the E-LAN service.

The SROS L2 packet cards support E-LAN, as illustrated in [Figure 15-2, “Ethernet LAN Service”](#) (p. 15-10).

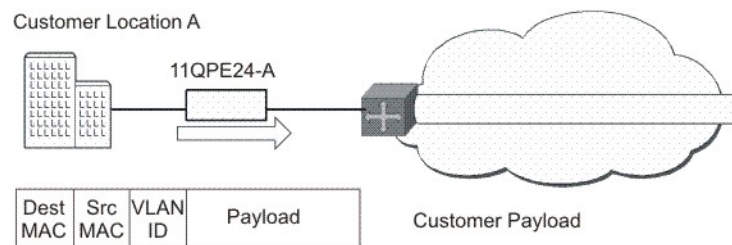
Figure 15-2 Ethernet LAN Service**E-LAN processing**

Note: In the following process, 11QPE24 is taken as an example for description and this feature is supported by 11DPE12(E/A), 11QPE24, and 11OPE8 cards.

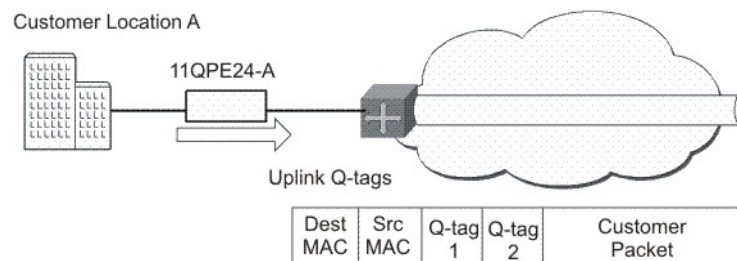
The following process describes E-LAN processing of a customer packet sent across the network from site-A, which is connected to NE-A through a DWDM network to Network Element C. This is a description of processing on the 11QPE24 bridges only, and does not include the processing on the DWDM network.

1. Service packets arriving at the 11QPE24 are associated with an E-LAN service based on the SAP type defined for the service. These can select all traffic (EP-LAN) or untagged, all VLAN-IDs, a single VLAN-ID, or all VLAN-IDs not associated with another SAP on the port.

Note: This implies support of both EP-LAN and EVP-LAN service types.



2. 11QPE24-A learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to the service access point (SAP) on which it was received.
3. The destination MAC address in the packet is looked up in the FIB table for the E-LAN instance. There are two possibilities: either the destination MAC address has already been learned (known MAC address) or the destination MAC address is not yet learned (unknown MAC address).
4. The packet is sent toward the network
 - If the destination MAC address has already been learned by the 11QPE24, an existing entry in the FIB table identifies destination uplink Q-in-Q SAP to be used for sending the packet towards the DWDM network.
 - If the destination MAC address has not been learned, the 11QPE24 will flood the packet to all SAPs in the service.



5. The DWDM network switches this packet and transports it across the core network to the remote DWDM-C1 NE.
6. The 11QPE24-C1 associates the packet with the E-LAN instance based on the VLAN tags in the received packet.
7. The 11QPE24-C1 learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to the uplink port, which the packet was received.
8. The destination MAC address in the packet is looked up in the FIB table for the E-LAN instance, and the packet is sent to it.

-
- If the destination MAC address has been learned by the 11QPE24, an existing entry in the FIB table identifies the local access port, or uplink port if the destination is at another node in the network, and the IEEE 802.1Q tag (if any) to be added before sending the packet to customer Location-C1. The egress Q tag may be different than the ingress Q tag, if so configured.
 - If the destination MAC address has not been learned, the 11QPE24 floods the packet to all the SAPs that are participating in the service.

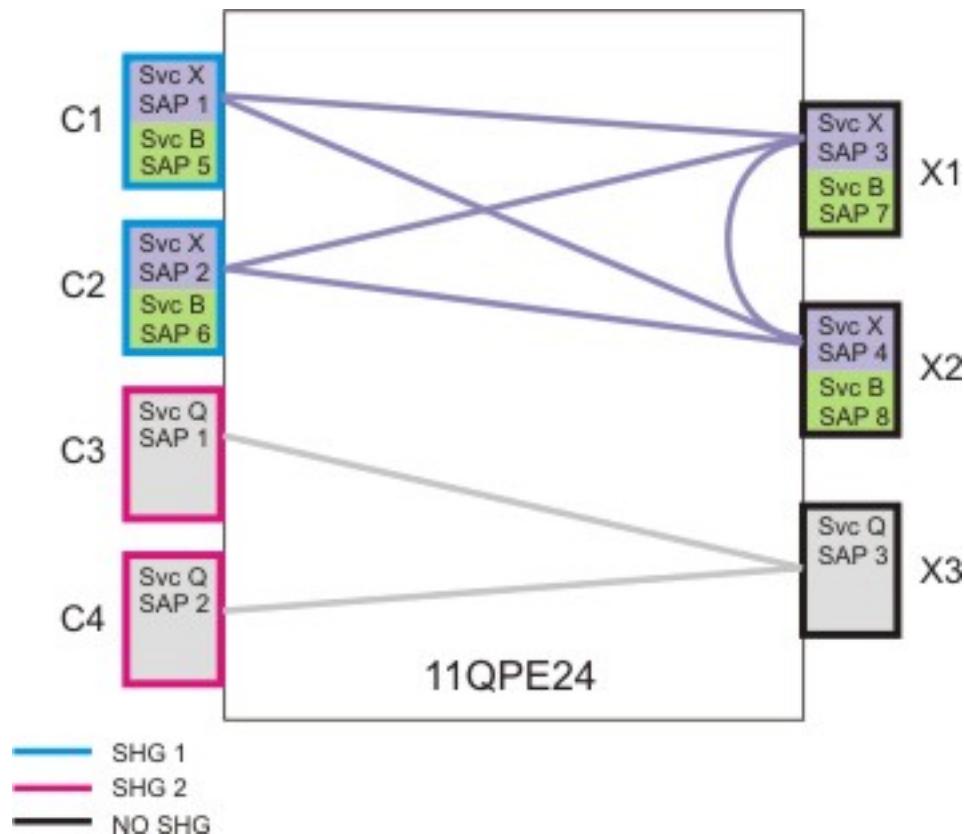
MEF E-Tree service

MEF 6.1 defines the service type, E-Tree (complementing E-Line and E-LAN). E-Tree consists of Roots and Leaves, and has the behavior of a Service containing SAPs not in an SHG (Roots) and in an SHG (Leaves). An E-Tree may be Private with one EP-Tree Service on the ports, which are null-encapsulated, or it may be Virtual Private where ports support other EVP-Trees or other VP Services.

MEF E-Tree service support (through SHG)

EP-Tree and EVP-Tree (rooted multipoint EVC), which are very popular MEF services for multicast service delivery, ISP access, mobile backhaul, can now be proposed. They are implemented through port-based Split-Horizon Group (SHG). SHG is as a group of ports which cannot communicate amongst themselves, but can pass traffic to other ports not members of the same SHG. Non-SHG ports are “roots” and the SHG ports are “leaves:” roots can speak to any port but leaves can only speak to the roots.

In the following illustration the blue SHG has two different services and two uplink ports (Virtual Private Trees). The red SHG has one service and one uplink port (null port/SAP -> Private Tree).



SAPs of different services on a port in an SHG are all subject to the traffic constraints of the SHG. Only SAPs in the same service and not in the same SHG can communicate among themselves. A service may have SAPs on some or all ports of one or more SHGs and some ports not in SHGs.

An E-Tree root may be on the same card as the leaves, or a different card. There may be more than one root in the network for redundancy.

The leaves of the E-Tree can only be configured on one card in the network to provide the required isolation. The leaf ports are in the same SHG and leaf SAPs are in the same Service as each other and the root(s).

E-Tree with ERP

An E-Tree is typically configured over ERP with leaf ports on one node and roots on one or more other nodes.

E-Tree with LAG

E-Tree leaves may be LAGs or individual ports or a mix. Roots may also be individual ports or LAGs. Roots may also be members of an MC-LAG.

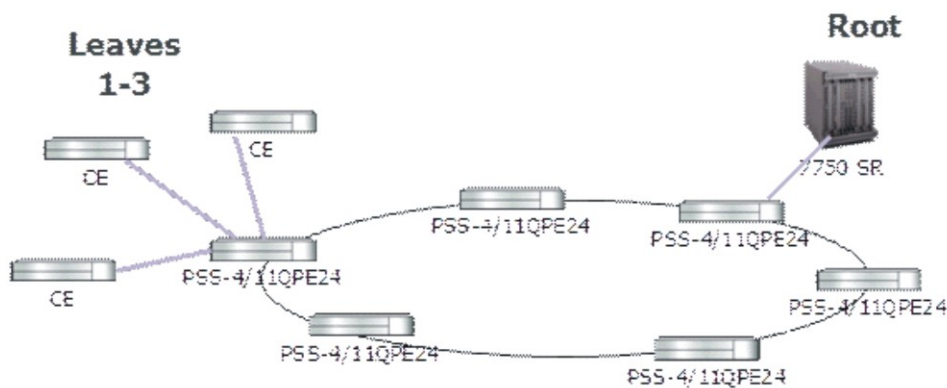
E-Tree with CFM

Monitoring an E-Tree normally consists of Up-MEPs on each root and leaf SAP in the same association. In this scenario the Up-MEPs on leaf SAPs do not exchange CCMs among themselves, only with the roots, the same as user traffic. On the card with the leaves the CFM association only has the roots listed as remote MEPs. On a card with a root, the association has the leaves and other root listed as remote MEPs. There is no need for CFM monitoring when roots and leaves are in the same card.

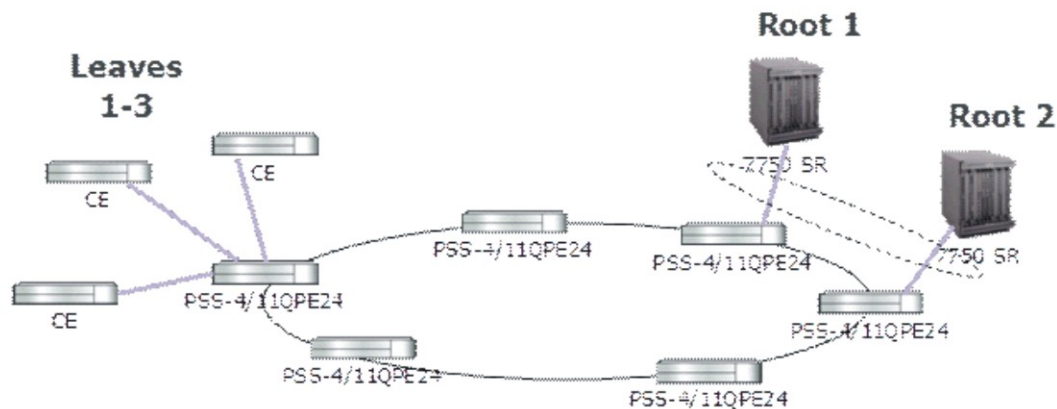
E-Tree application scenarios

The following illustrations show different scenarios for E-Tree applications.

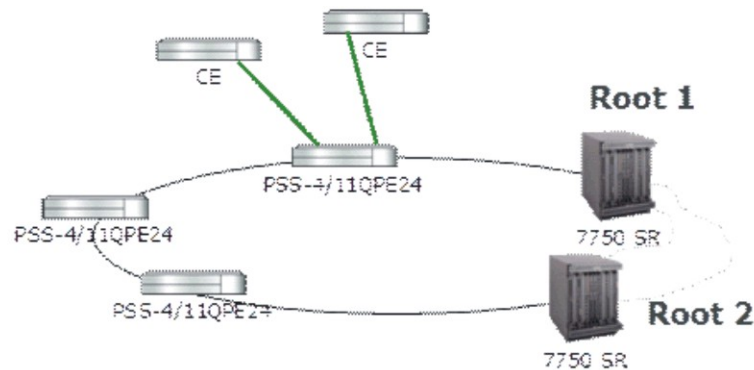
Figure 15-3 E-Tree with single remote root



- Single Root
- Root and Leaves are in the same VPLS Service over ERP
- Leaves are in one SHG
- Multiple E-Tree Services on same Leaf ports can be configured

Figure 15-4 E-Tree with redundant remote roots

- Roots may be members of an MC-LAG (dotted line)

Figure 15-5 E-Tree with dual homed roots

- Two Roots for redundancy which decide among them which one is active
- Dual homed open ring (ERP subring without virtual channel)
- Roots and Leaves are in the same VPLS Service over ERP
- Leaves are in one SHG
- Multiple E-Tree Services on same Leaf ports can be configured

MEF CE-VLAN bundling (VLAN range SAP)

VLAN ranges provide a mechanism to group a range of VLAN IDs as a single service entity. This allows the operator to provide the service treatment (forwarding, ACL, QoS, PM, and others) to the group of VLAN IDs as a whole.

This feature is supported in both access uplink mode and in MPLS-TP mode.

Note: IGMP snooping is not supported on VLAN range SAP.

CE-VLAN bundling is supported on the SROS L2 packet cards.

Connection-profiles are used to create or specify the VLAN range values to be used by the access SAPs. It is possible to specify ranges of VLAN IDs and/or individual VLANs to be grouped together in a single SAP.

VLAN range SAPs restrictions

The following restrictions apply for the VLAN range SAPs:

- The system allows only one range SAP in a VPLS service. It will fail any attempt to configure more than one range SAP in a service.
- The dot1q range SAP can be configured only on access ports.
- The dot1q range SAP is allowed to be configured only in a service with svc-sap-type set to "dot1q-range".
- The access SAPs using VLAN range values are allowed only for Dot1q encapsulation port or LAG with Dot1q encapsulation.
- No Dot1q default SAP is allowed on the same access port as the one on which a SAP with a range is configured.
- Access-uplink SAPs used in a dot1q-range service must all be of the Q1.* SAP type.
- Multiple "connection-profiles" can be used per port or Lag as long as the VLAN value specified by each of them does not overlap. The number of VLAN ranges available per port/LAG is limited. The available number must be shared among all the SAPs on the port/LAG.
- A maximum of up to 8 VLAN ranges are allowed per connection profile.
- "Connection-profile", associated with a SAP cannot be modified. To modify a connection profile, it must be removed from all SAPs that are using it.

OAM for Range SAPs

Ethernet CFM works the same way on the VLAN range bundle as any other service. A MEP monitors the service (bundle), not individual members of the bundle. One CVLAN from the range of CVLANs is designated as primary VLAN to represent the bundle. Its value is configured in CLI using the "**vlan**" parameter in the eth-cfm>domain>association>bridge-identifier context. The value of 0 for the primary VLAN means no CVLAN is used by the MEP.

The VLAN of the bridge-identifier context becomes the primary VLAN by the primary-vlan-enable parameter on the dot1q-range SAPs' MEP. It is used as the CVLAN tag in the packet header for egressing CFM messages of the MEP.

CFM OAM is supported for Up MEPs on the dot1q range SAP. When the primary VLAN value is 0, the CFM frames egressing the uplink SAP are SVLAN-tagged.

A Down MEP is supported on a dot1q-range SAP. When the primary VLAN is 0, the CFM messages are untagged.

Note: MIPs are supported when the primary VLAN is 0, and the intermediate SAP is of type Q1.*, using only the SVLAN tag.

VLAN for Range SAPs

Filter policies are supported on dot1q range SAP ingress. IPv4/v6 criteria and MAC criteria based filter policy are expected to be supported with access SAPs.

Ingress classification, metering with hierarchical metering, marking, queuing and shaping for SAP ingress and SAP egress are supported. On egress per port queues and shaping is also supported.

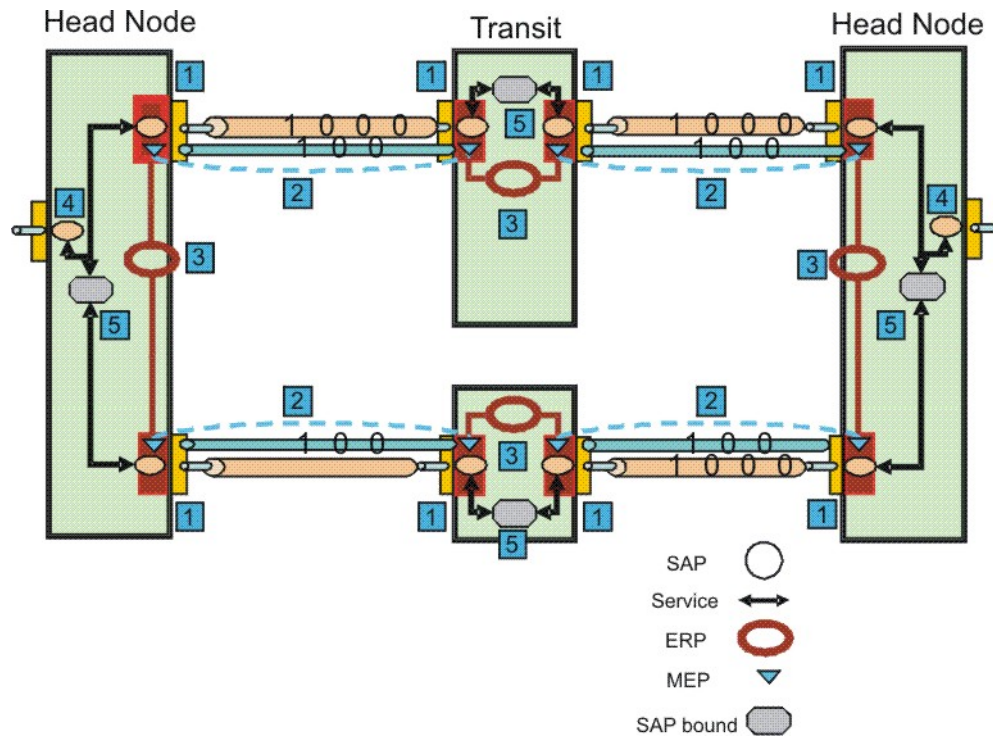
Ingress accounting support is similar to the support available for other SAPs. Count of packets or octets received per individual VLANs configured in the connection profile is not available. No support for Egress SAP statistics and accounting is available.

The use of service resiliency mechanisms such as MC-LAG redundancy and ERP is supported on service with dot1q range SAPs.

Ethernet ring protection (ERP)

Ethernet ring protection (ERP) switching offers ITU-T G.8032 specification compliance to achieve resiliency for Carrier Ethernet networks. Because it is simple, robust, and optimized for rings, it is faster and more reliable than, and therefore preferred over, IEEE 802.1 Spanning Tree Protocols in ring networks. Similar to STP networks, ERP normally keeps one link in the ring blocked to user traffic, but also like MSTP, it is possible to run multiple ring sessions on the same physical ring, with different blocked links in each. This enables load balancing on the ring when traffic patterns allow.

Protected Ethernet service, using Ethernet Ring Protection (ERP), is also supported as shown in the following figure.

Figure 15-6 Protected Ethernet service

The following steps provide a general outline of the procedure to create the protected service shown above.

1. Configure the ports
2. Configure the ETH OAM infrastructure
3. Provision ERP
4. Create the services, SAPs, and Down MEPs for the ring
5. Create the services and SAPs bound to the ring for customer

Eth-rings can interwork with other Eth-rings with single or dual interconnections. In Release 6.0, only E-LAN services can use ERP (e-pipes are emulated as two-node ERPs). All E-LAN services may be protected by one Eth-ring instance, or arbitrarily divided among several.

ERP is instantiated on uplink (NNI) ports, and ERP switching is triggered by NNI port failures, and also optionally by Eth-OAM CCM link faults detected by Down MEPs on the ring ports, for a ring topology in which links are not directly connected. Although ring switching can be held off to allow underlying protection to operate first, this is not usual: the advantage of ERP is its native fast (~50 ms) protection switching.

Eth-rings use the G.8032 standard protocol for control, and participating nodes exchange protocol messages using Y.1731-defined OAM frames called R-APS. R-APS frames are sent by MEPs belonging to an MA not associated with a service, and positioned on ring paths. R-APS frames are tagged and should be configured with a unique VID (that is not shared with a service or other ring) when the ring port has dot1q encapsulation. R-APS frames are tagged with a unique outer VID when the ring port has Q-in-Q encapsulation (the inner VID does not matter). In Release 6.0, Eth-rings are only on individual ports (no LAGs).

In the 1830 PSS implementation, the Ethernet Ring control instance is built from a dedicated dummy VPLS service on each node with VPLS SAPs that carries only R-APS messages. It is not used for subscriber data.

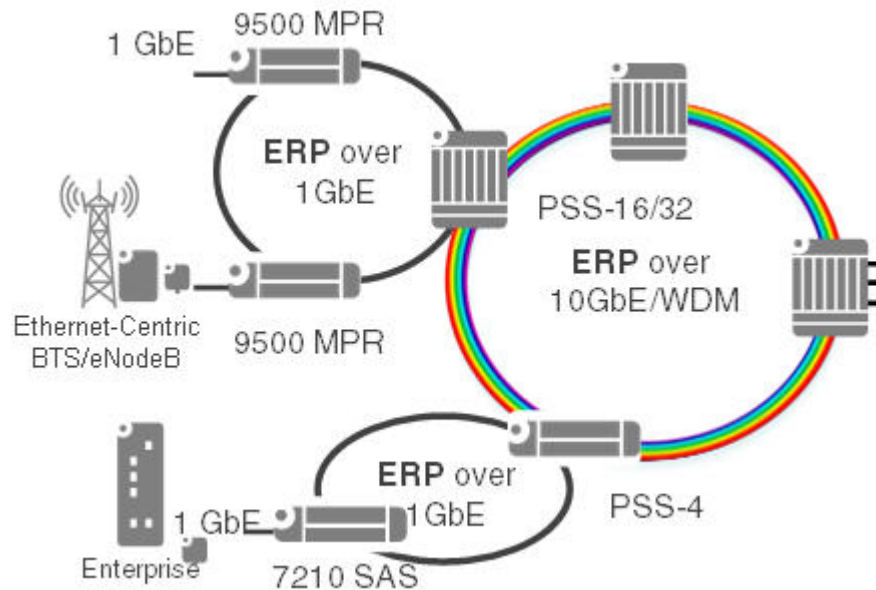
G.8032 terminologies

The following is a list of G.8032 terminologies that is used in the following sections.

- **Ring Protection Link (RPL):** Link designated by mechanism that is blocked during Idle state to prevent loop on bridged ring
- **RPL Owner:** Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protected state
- **Link Monitoring:** Links of ring are monitored using standard ETH CC OAM messages (CFM)
- **Signal Fail (SF):** Signal Fail is declared when ETH trail signal fail condition is detected
- **No Request (NR):** No Request is declared when there are no outstanding conditions (for example, SF, and so on.) on the node
- **Ring APS (R-APS) Messages:** Protocol messages defined in Y.1731 and G.8032
- **Automatic Protection Switching (APS) Channel:** Ring-wide VLAN used exclusively for transmission of OAM messages including R-APS messages

ERP on 1G UNI & NNI and 10G UNI ports

ITU-T G.8032 can also be configured on 1G NNI (uplink) ports with Q-in-Q encapsulation, and on 1G and 10G UNI (access) ports, only for dot1Q and Q-in-Q encapsulation. This allows interworking on Ethernet interfaces in access rings with systems also supporting G.8032(v2) such as 7210 SAS-M, 9500 MPR, ISA-ES, Omniswitch. The number of ERP instances is also increased to 32 per card.

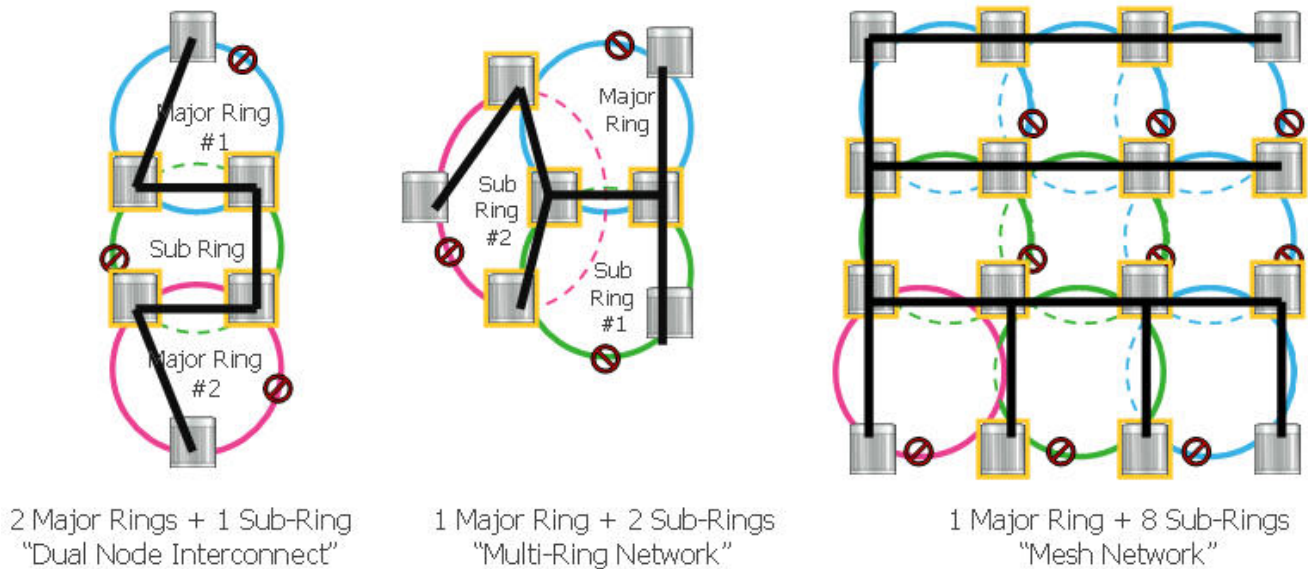
Figure 15-7 ERP over 1 GbE UNI and NNI ports and 10 GbE UNI ports**ERP Ring Interconnection with DNI using Sub-Rings**

The Major/Sub-ring model of ITU-T G.8032(v2) is implemented and allows ring interconnection through a pair of nodes, offering a very scalable, flexible and resilient ring interconnection that protects against simultaneous failures (one per ring) and protects against failure of the interconnection nodes.

As illustrated in the following, any given network without open ends can be represented as a single Major Ring with one or more Sub-Rings attached.

The Sub-Ring model without R-APS Virtual Channel is implemented in Release 6.0 as it requires less configuration, allows to reuse VLAN Ids for R-APS control channel and allows dual-ended open rings.

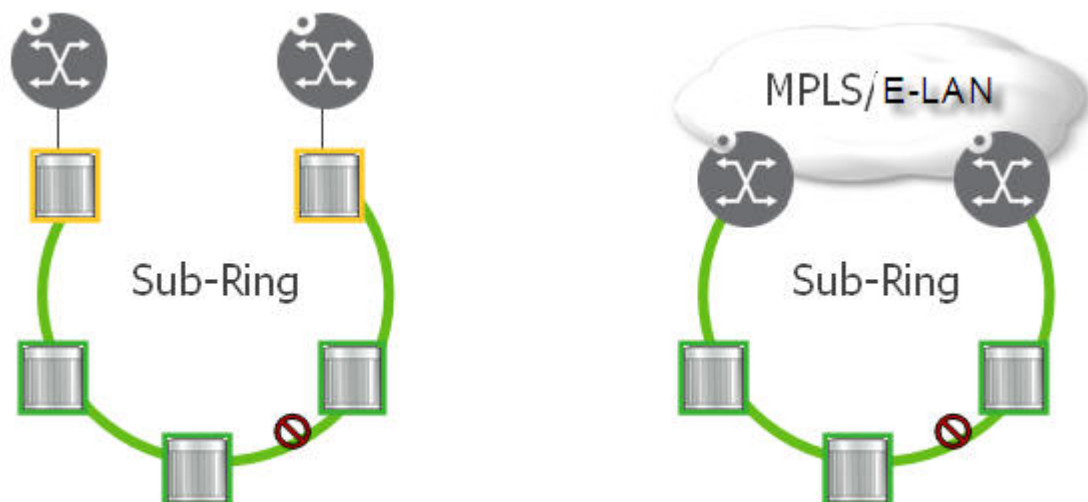
Figure 15-8 ERP Major/Sub-ring examples



The following sections describe ERP Sub-ring applications:

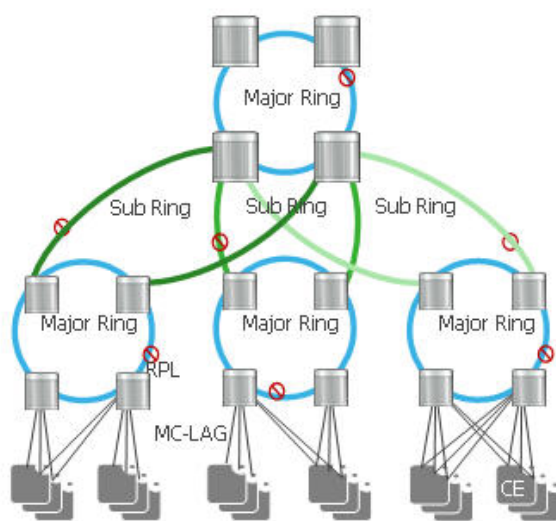
Dual-Home Open Ring - With the mode without R-APS Virtual Channel, dual-homed open rings or dual-homing into MPLS/VPLS can be supported, as illustrated in the following:

Figure 15-9 ERP Sub-ring applications: Dual-Home Open Ring

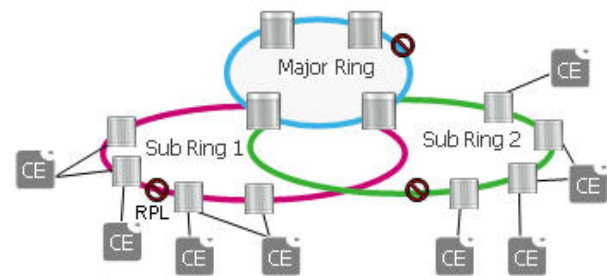


Multiple ring hierarchy, Collapsed rings and Interconnection into E-LAN - For Multiple Ring Hierarchy virtual channel is needed, otherwise sub-rings would be isolated. Interconnection into E-LAN only works with non-virtual channel.

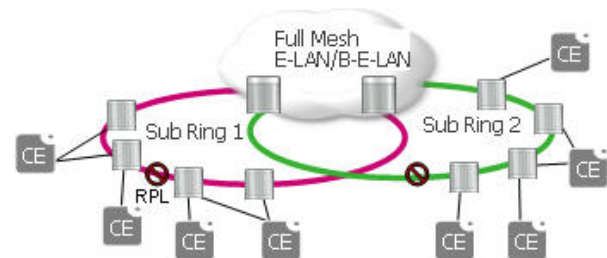
Figure 15-10 ERP Sub-ring applications: Multiple ring hierarchy, Collapsed rings and Interconnection into E-LAN



Multiple Ring Hierarchy
(virtual channel is needed, otherwise sub-rings would be isolated)



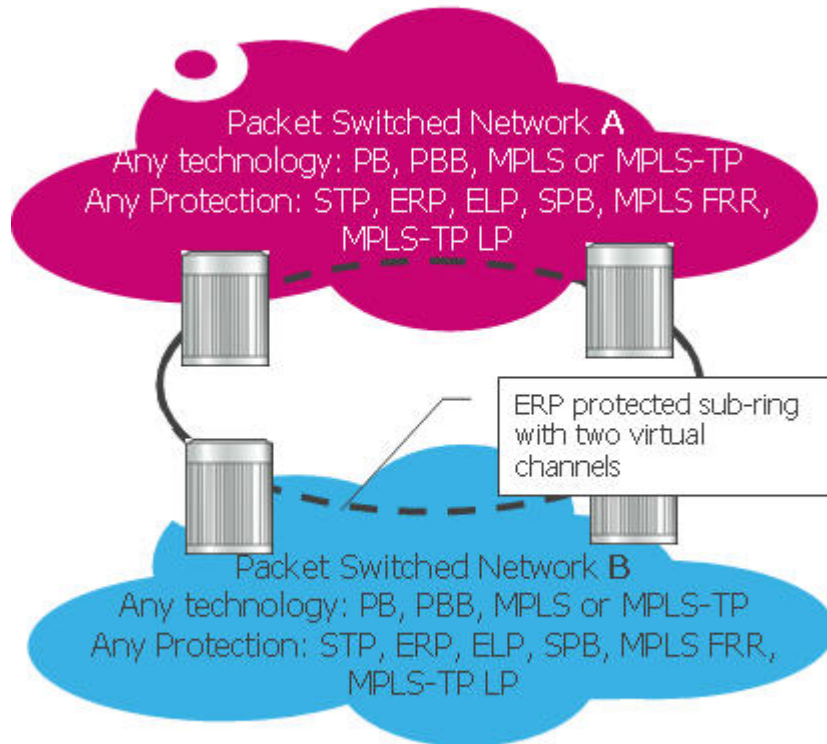
Collapsed Rings



Interconnection into E-LAN
(only works with non-virtual channel)

ERP Sub-ring applications: Dual Node Interconnection of different Packet-Switched Networks - ERP allows to interconnect two networks in a fully redundant manner, even if those networks operate in different switching technologies or use different protection schemes. Interconnection nodes need to support ERP. The virtual channel can be tunneled through other native technologies in the interconnected networks.

Figure 15-11 ERP Sub-ring applications: Dual Node Interconnection of different Packet-Switched Networks



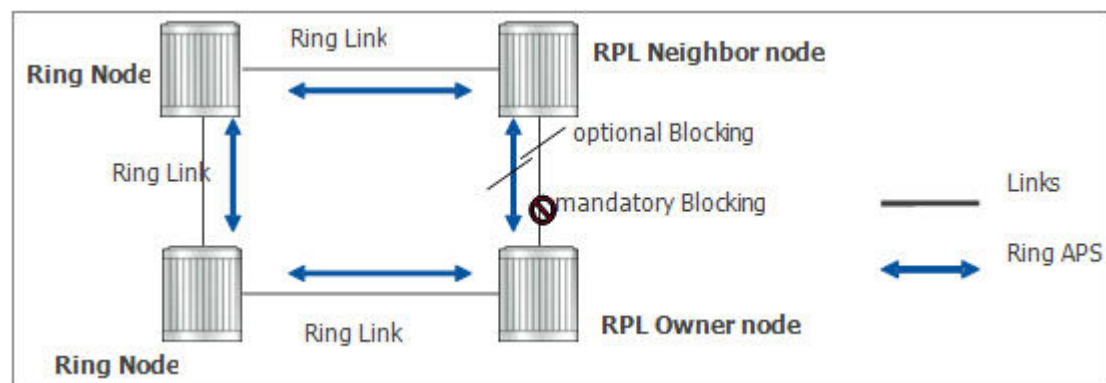
G.8032 ERP protocol

R-APS messages that carry the G.8032 protocol are sent on a dedicated protocol VLAN called ERP VLAN (or Ring Control Instance). In the revertive case, and initially in the non-revertive case, G.8032 Protocol ensures that the Ring Protection Link (RPL) owner blocks the RPL link. R-APS messages are periodically multicast in both directions to simultaneously inform other nodes in the Ring about the blocked port in the RPL owner node. In non-revertive mode any link may be the blocked link; it is the last one to recover from a failure. Revertive operation ensures a known configuration and is required when multiple concurrent rings are used for load balancing. Non-revertive operation avoids the extra traffic hit caused by reversion. Y.1731 Ethernet OAM APS is the basis of the R-APS messages. Y.1731 CC messages are typically used by nodes in the ring to monitor the health of each link in the ring in both directions. However CC messages are not mandatory. Other link layer mechanisms are considered - for example Ethernet LOS (Loss of Signal) when the nodes are directly connected.

Ring Start-up convergence

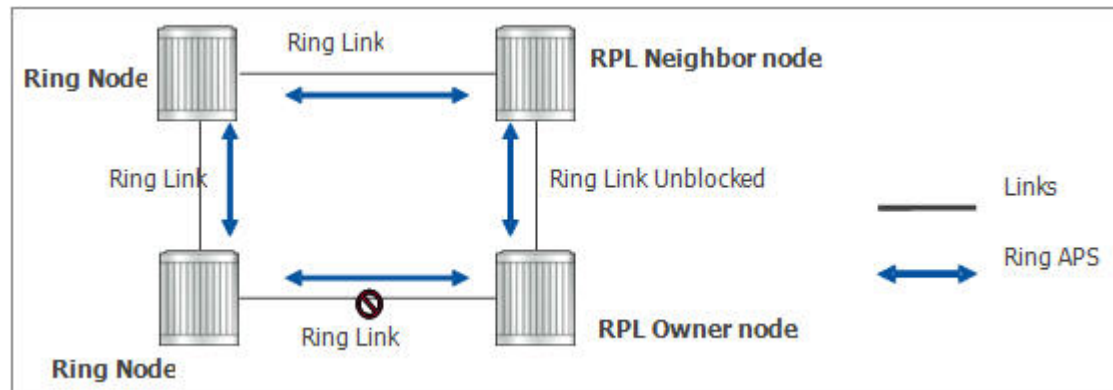
Initially each Ring Node blocks one of its links and notifies other nodes in the ring about the blocked link (RPL Owner blocks the RPL). Once a ring node in the ring other than the RPL Owner learns that another link is blocked, the node unblocks its blocked link. This possibly causes a FDB flush in all links of the ring for the affected service VLANs. This procedure results in unblocking all links but the RPL and the ring normal (or idle) state is reached. In revertive mode, the RPL link is always the link that is blocked when all links are operable after the revert (WTR) time. In non-revertive mode, the RPL link is no different from other ring links (until a clear command is issued, which restores the RPL as blocked). Each time there is a topology change that affects reachability, the nodes flush their FDB and MAC learning takes place for the affected service VLANs. This allows forwarding of packets to continue, some on new paths. Flushing is triggered by the G.8032 state machine and the 11QPE24 implementation allows flooding of traffic during the flushing interval to expedite traffic recovery. See [Figure 15-12, “G.8032 Ring in the initial state”](#) (p. 15-24) that depicts this operational state. **Note:** The blocked link is transparent to R-APS.

Figure 15-12 G.8032 Ring in the initial state



Ring fault operation

When a ring failure occurs, the node or nodes detecting the failure (by local port fault or by Y.1731 OAM CC monitoring) send R-APS message in both directions. This allows the nodes at both ends of the failed link to block forwarding to the failed link and preventing it from being active. In revertive mode, the RPL Owner (or in non-revertive mode, whichever node(s) are blocking) then unblocks the previously blocked RPL and triggers FDB flush for all nodes for the affected service instances by R-APS. The ring is now in the protecting state and full ring connectivity is restored. MAC learning takes place to allow Layer 2 packet forwarding on a ring. The following [Figure 15-13, “G.8032 Ring in the Protecting State”](#) (p. 15-25) depicts the failed link scenario.

Figure 15-13 G.8032 Ring in the Protecting State**Ring fault recovery**

Once the failed link recovers, the nodes that blocked the link again send the R-APS messages indicating no failure this time. This in turn triggers the RPL Owner to block the RPL link (following Wait-to-Restore time-out) and indicate the Blocked RPL link the ring in R-APS message, which when received by the nodes at the recovered link cause them to unblock that link and restore connectivity (again all nodes in the ring perform FDB Flush and MAC learning takes place). In non-revertive mode the RPL ignores the messages from the nodes with blocked links, and they remain blocked; no FDB flushing is needed. The ring is back in the normal (or idle) state.

Timers

The user can configure the guard and revert timers. The guard timer is used to prevent stale R-APS messages, circulating after a local Signal Fail clears, from affecting the state machine. It may need to be tuned to optimize for different size rings. The revert timer, also known as Wait to Restore (WTR), is only effective in revertive mode, and enforces delay to allow “bouncing” faults to settle before the RPL owner reverts to the normal blocked state. There is a non-configurable Wait to Block (WTB) timer used by the RPL owner to delay reversion to the blocked state following the removal of an operator switch command. This is to ensure there is no other forced switch on the ring.

ERP hold-off timer

Hold-off timer supports the lower layer switchover to protection or restore before the ETH layer. Hold-off timer ensures server layer protection switches before ERP when SROS L2 packet cards are cascaded with other transponders implementing optical layer protection or using GMPLS at L0.

Hold-off Timers are used by the underlying ETH layer to filter out intermittent link faults. Faults will be reported to the ring protection mechanism if this timer expires. The port Hold-off timer is used to reduce the number of link transitions that are reported to the upper layer protocols.

If the provisioned hold-off timer value is non-zero, when a new defect or more severe defect occurs, this event is not reported immediately to the system. Instead, the hold-off timer is started. When the hold-off timer expires, the trail that started the timer is checked as to whether a defect still exists. If a defect exists, that defect is reported to protection switching.

Note: The reported defect need not be the same defect that started the timer.

Use of ETH-CFM MEPs

Within each path, Y.1731 Down MEPs are used to exchange R-APS specific information (when “control-mep” is enabled). For this function, the Down MEPs behave more like MIPs than standard Down MEPs. The Down MEPs copy and forward received R-APS PDUs, and terminate them only if they originated locally. This allows faster propagation of information than hop-by-hop signalling as is done by spanning tree protocols.

The MEPs can also optionally exchange fast CCM for node-to-node fault detection. This is necessary, when nodes are not directly connected by Ethernet links so that not all faults are detected by the ports. CCM messages can be configured with intervals between 3.3 msec and 100 msec, the former providing fault detection time of 10 msec.

Because the path Down MEP is monitoring the link, and not a service, it is typically configured at a low MD level, although this is not required. The control tag (raps-tag) defined under each Eth-ring path is used by the MEP for encapsulating and forwarding the CCMs and the G.8032 R-APS messages used for the protection function.

Fault detection

For fault detection using CCMs, three CC messages must be missed for a fault to be declared on the associated path. After it receives the fault indication, the protection module declares the associated ring link down and the G.8032 state machine sends the appropriate messages to open the blocked link and flush the learned addresses.

Service allocation to Ring instances

G.8032 supports multiple data channels (services) per ring control instance (R-APS tag). G.8032 also supports multiple control instances such that each instance can have its RPL on a different link providing for a load balancing capability. However once services have been assigned to one instance, the same services on other nodes must be on the same ring instance. When there is any one link failure or any one node failure in the ring, the G.8032 protocol is capable of restoring traffic among all remaining nodes for these data services.

Each NNI (uplink) port supports up to six ring instances, which can coexist with unprotected VPLS SAPs.

Rings on UNI (Access) ports

Ethernet R-APS can be configured on any UNI (1 Gb or 10 Gb) access ports configured using dot1q, Q-in-Q encapsulation. This enables support for Ethernet R-APS protected services on the service edge towards the customer site.

Rings on NNI (access uplink) ports

Ethernet R-APS can be configured on any NNI (10 Gb) X port access uplink configured using Q-in-Q encapsulation enabling support for Ethernet R-APS protected services on the service within the Ethernet backbone.

In Release 6.0, Ethernet R-APS can also be configured on any NNI (1 Gb) C port access uplink, configured using Q-in-Q encapsulation. This enables support for Ethernet R-APS protected services on the service within the Ethernet backbone. This is mainly used to create Sub-Rings on C port attached to major Rings on X port, all for NNIs.

Service independence from Ring

E-Line, E-LAN services can be given Ethernet R-APS protection and the services are configured independent of the Ring properties. The intention of this is to cause minimum disruption to the service during Ethernet R-APS failure detection and recovery. **Note:** E-Line services are provided using the VPLS service construct because E-pipes are not currently supported by ERP.

QoS considerations

Ethernet ring CC and R-APS messages transmitted over the SAP queues using the default egress QoS policy use NC (network class) as a forwarding class. If user traffic is assigned to the NC forwarding class, it competes for the same bandwidth resources with the Ethernet CCMs. As CCM loss could lead to unnecessary switching of the Ethernet ring, congestion of the queues associated with the NC traffic should be avoided. The operator must configure different QoS Policies to avoid congestion for the CCM forwarding class by controlling the amount of traffic assigned into the corresponding queue. For the same reason, the **ccm-ltm-priority** setting for the control MEPs should always be the highest priority.

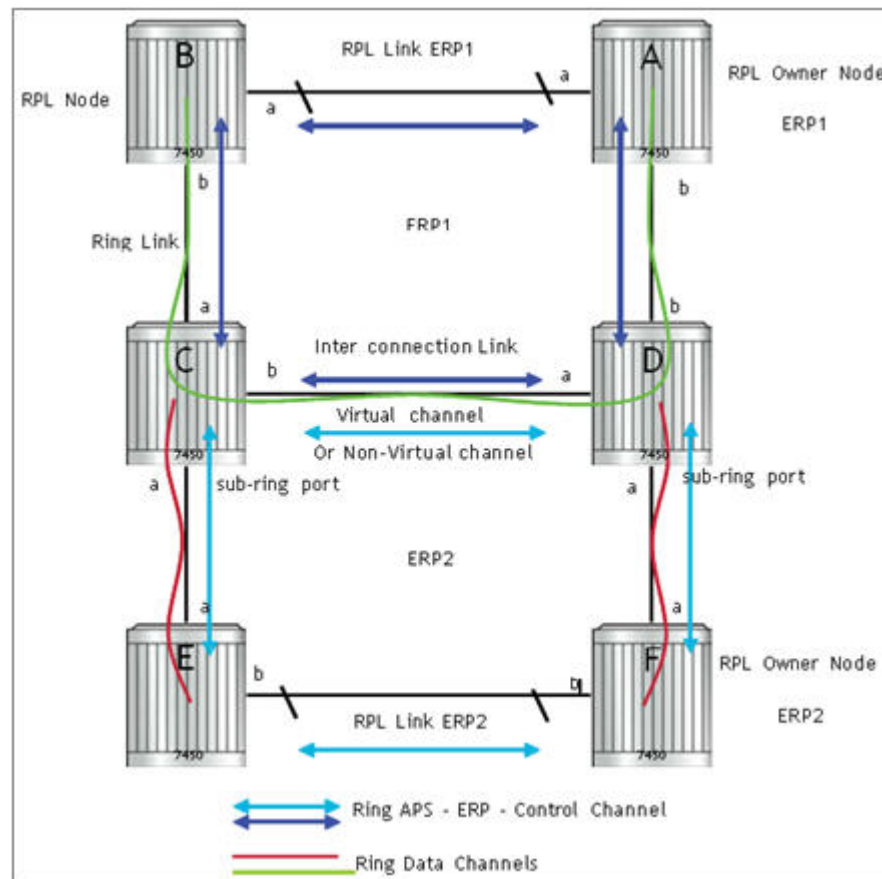
Operator switch commands

The user can control ring switching by commands in the **tools > perform > eth-ring** context. The **force** command puts the target path into the blocked state, which remains regardless of faults or other force commands in the ring. Unless otherwise constrained (fault or force), the RPL owner removes its block at that time. The **manual** command is similar, except that the block remains only while the ring is fault-free. The **clear** command, which applies to the ring instance, removes either of the above local commands. In the revertive mode, it also clears an active WTR or WTB timer to cause immediate reversion; in the non-revertive mode it causes reversion to the RPL owner.

Ethernet sub-rings

Ethernet Sub-Rings offer a dual redundant way to interconnect rings. 11QPE24 supports sub-rings connected to major rings and a sub-ring connected to a VPLS (Router based). The following [Figure 15-14, “Ethernet sub-ring” \(p. 15-28\)](#) illustrates a Major ring and Sub Ring scenario. In this scenario, any link can fail in either ring (ERP1 or ERP2) and each ring is protected. Furthermore, the sub ring (ERP2) relies on the major Ring (ERP1) as part of its protection for the traffic from C and D. The nodes C and D are configured as inter connection nodes.

Figure 15-14 Ethernet sub-ring



Sub-Rings and Major Rings run similar state machines for the ring logic, however there are some differences. When Sub-Rings protect a link, the flush messages are propagated to the major ring. (A special configuration allows control of this option on the 11QPE24). When major rings change topology, the flush is propagated around the major ring and does not continue to any sub-rings. The reason is that Major Rings are completely connected but Sub-Rings are dependent on another ring or network for full connectivity.

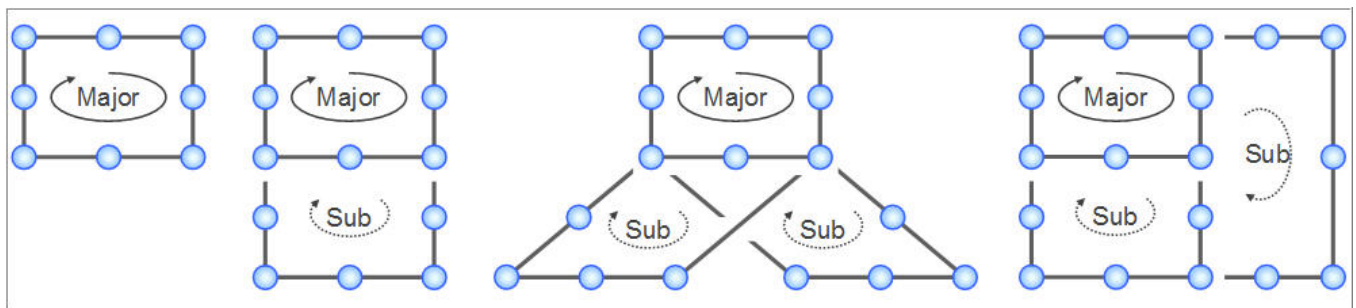
The topology changes need to be propagated to the other ring or network usually. Sub-Rings offer the same capabilities as major rings in terms of control and data so that all link resource may be utilized.

Multi-ring topologies

Major rings and Sub-rings can be used to build a nested infrastructure.

- Major ring and sub ring can interconnect
- Sub ring and Sub ring can interconnect
- Major rings cannot interconnect

Figure 15-15 Nested rings



Virtual and non-virtual channel

The 11QPE24 supports both the virtual channel and non-virtual channel for Sub-Ring control communication. In the virtual channel mode, a dedicated Sub-Ring VID, other than the Major Ring RAPs control channel is configured as a data instance on the Major Ring. This allows the Sub-Ring control messages and state machine logic to behave similar to a major ring. In the non-virtual channel mode, the sub-ring is only connected by the RAPs control channels on the sub-ring itself. This mode offers slightly less redundancy in the RAPs messaging than the virtual channel mode since Sub-Ring RAPs messages are not propagated across the major ring. When non-virtual link is configured, the protocol allows RPL messages over the Sub-Ring blocked link (RPL Neighbor is not used).

Sub-Ring configuration is similar to Major Ring configuration and consists of three parts:

- Eth-ring instance configuration
- Control VPLS configuration
- Data VPLS configuration (data instance or data channel)

The Eth-ring configuration of a Sub-Ring is tied to a major ring and only one path is allowed. **Note:** In Virtual Channel Sub-Ring, a split horizon group is mandatory to ensure that Sub-Ring control messages from the major ring are only passed to the Sub-Ring control.

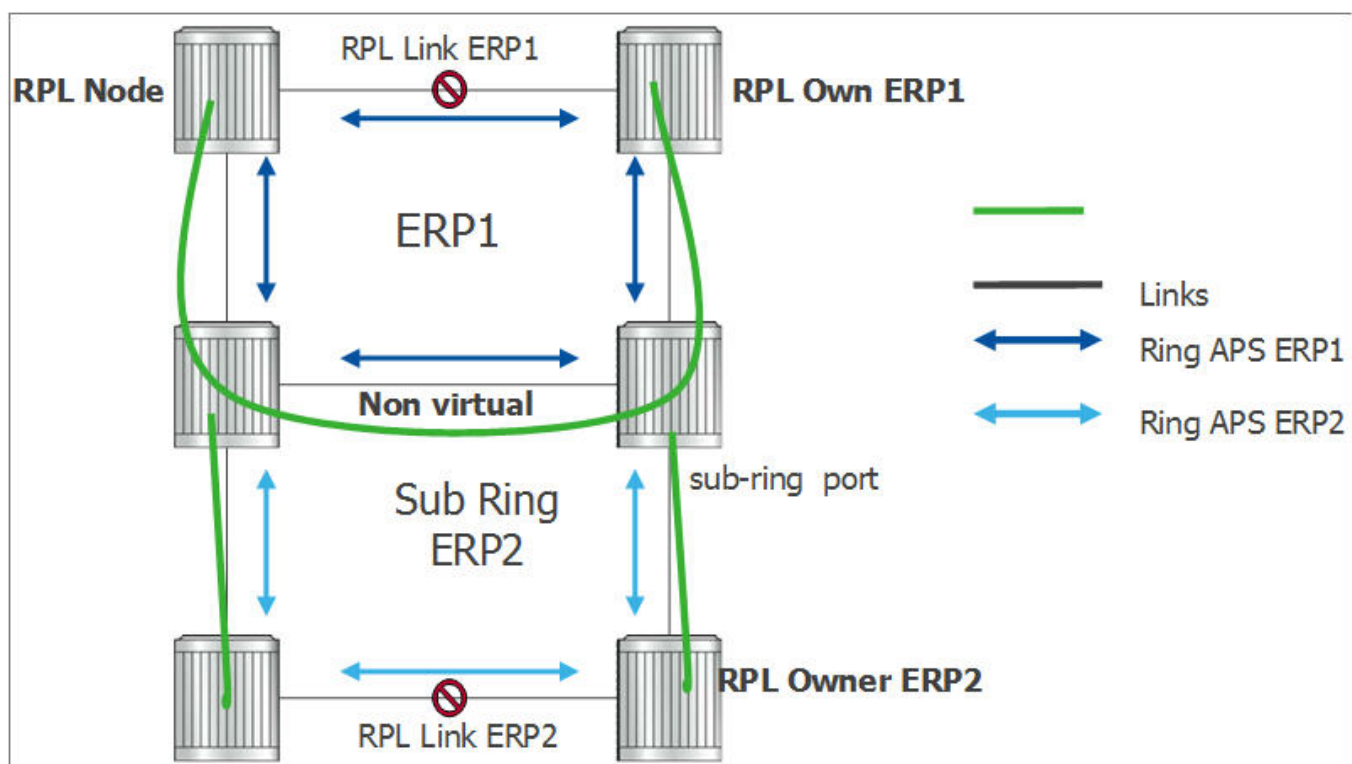
The Data VPLS can be configured on the major ring, and in the example, shares the same VID (SAP encapsulation) on both the Major Ring and the Sub-ring to keep data on the same VLAN ID everywhere.

Note: As like any other services in the 11QPE24, the encapsulation VID is controlled by SAP configuration and the association to the controlling ring is by the Eth-ring ring-id.

Major ring with a non-virtual sub-ring

The following figure illustrates a sample for a Major Ring with a Non-Virtual Sub-Ring configuration:

Figure 15-16 Major ring with non-virtual sub-ring



Since the Sub-Ring is configured as a non-virtual-link, the Sub-Ring configuration uses the “non-virtual-link” keyword in CLI. The Major Ring that the Sub-Ring is part of, is identified using the “interconnect” keyword. **Note:** On the interconnecting node “D”, only one Eth-ring path is created for the Sub-Ring. No R-APS messages are sent between node “D” and “C” for the Sub-Ring.

Figure 15-17 Sub-ring Eth-ring creation

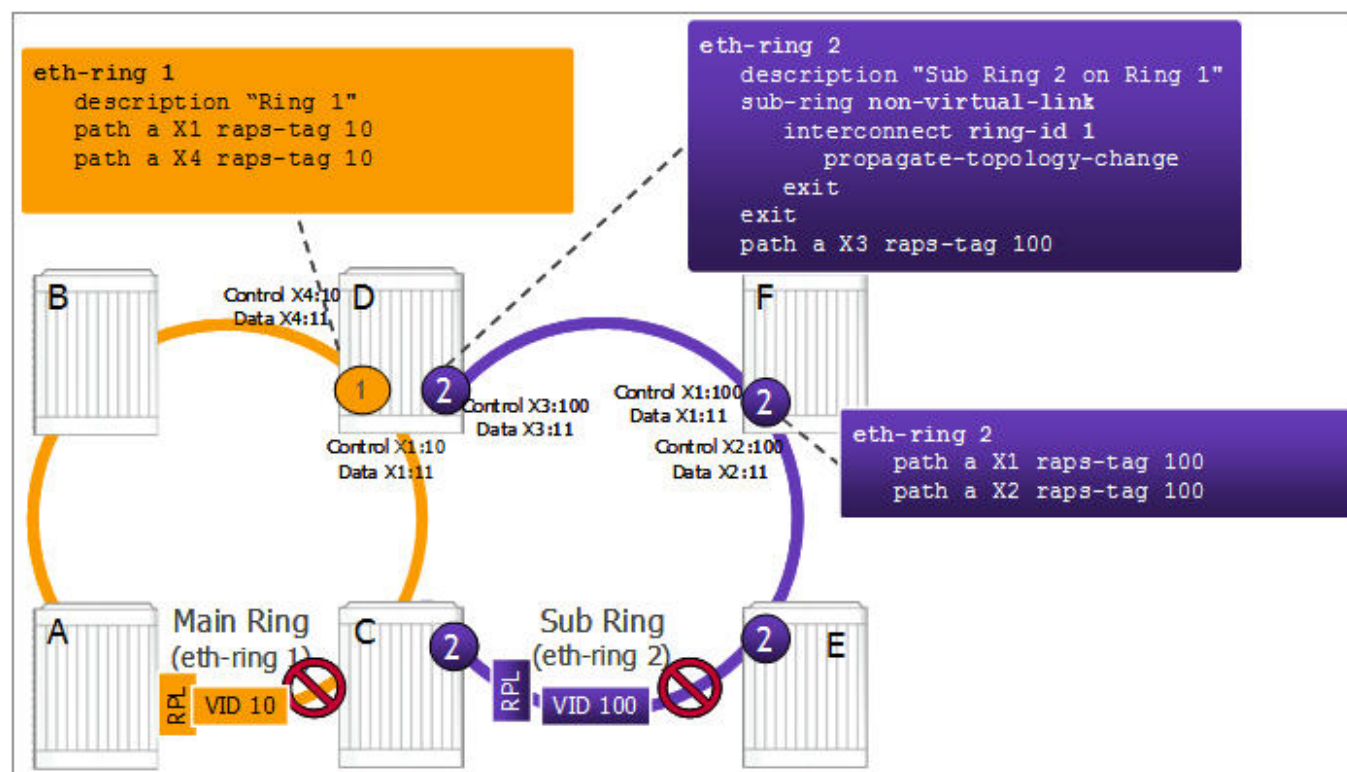
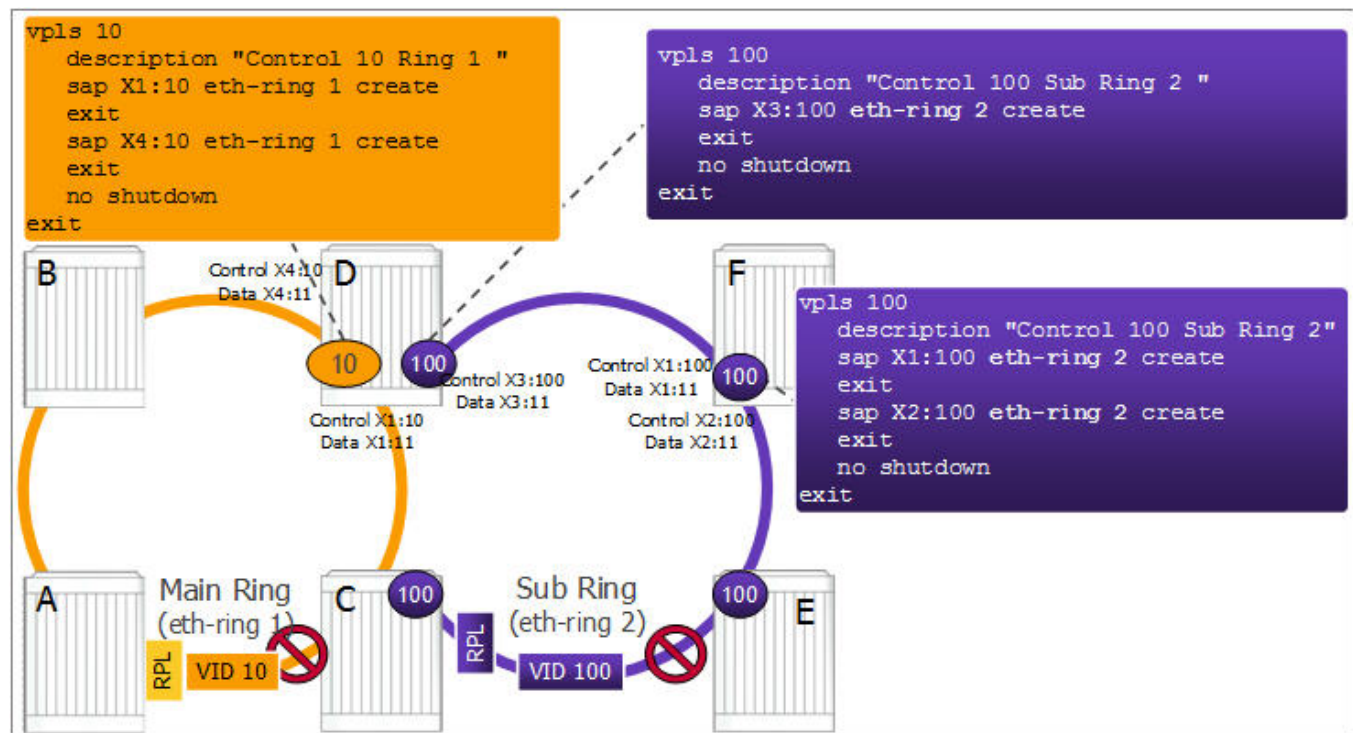
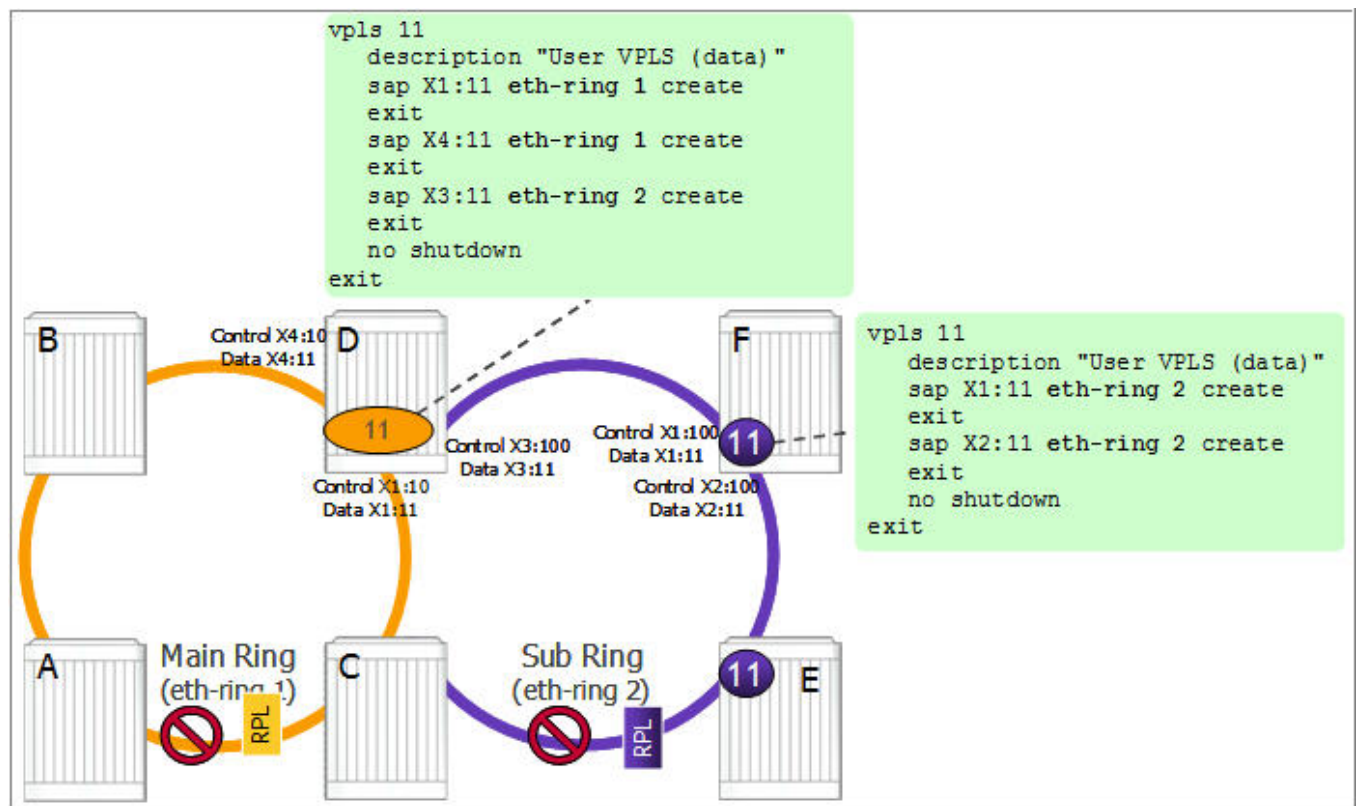


Figure 15-18 Sub-ring control creation



See the following figure for an illustration of Data VPLS creation for Ring and Sub-Ring

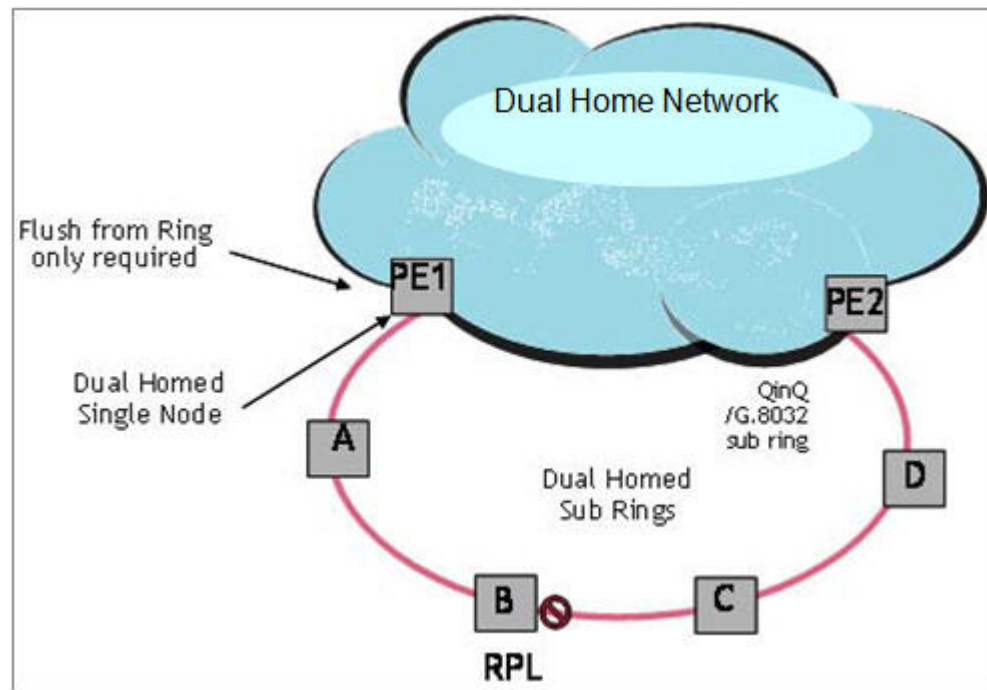
Figure 15-19 Data VPLS creation



Non-virtual sub-ring dual homed

The following [Figure 15-20, “Dual Homed sub-ring”](#) (p. 15-34) shows an example of Non-Virtual Sub-Ring connected to a Dual Home configuration.

The primary application is for access rings that require resiliency in the network. ERP control VPLS is used to terminate/switch Ring Control (R-APS), Router based services terminates the Ring Data on PE1 and PE2.

Figure 15-20 Dual Homed sub-ring

Since the Sub-Ring is configured as a non-virtual-link, the Sub-Ring configuration uses the “non-virtual-link” keyword in CLI. No Major Ring is defined in a dual Homed network. **Note:** On the node “A, B, C, and D, Sub-Ring will be configured as normal open Sub-Ring. The interconnection on the Sub-Ring to the Cloud/VPLS is done on the PEs Node, which does not include the 11QPE24.

Figure 15-21 Dual Homed Sub-ring creation

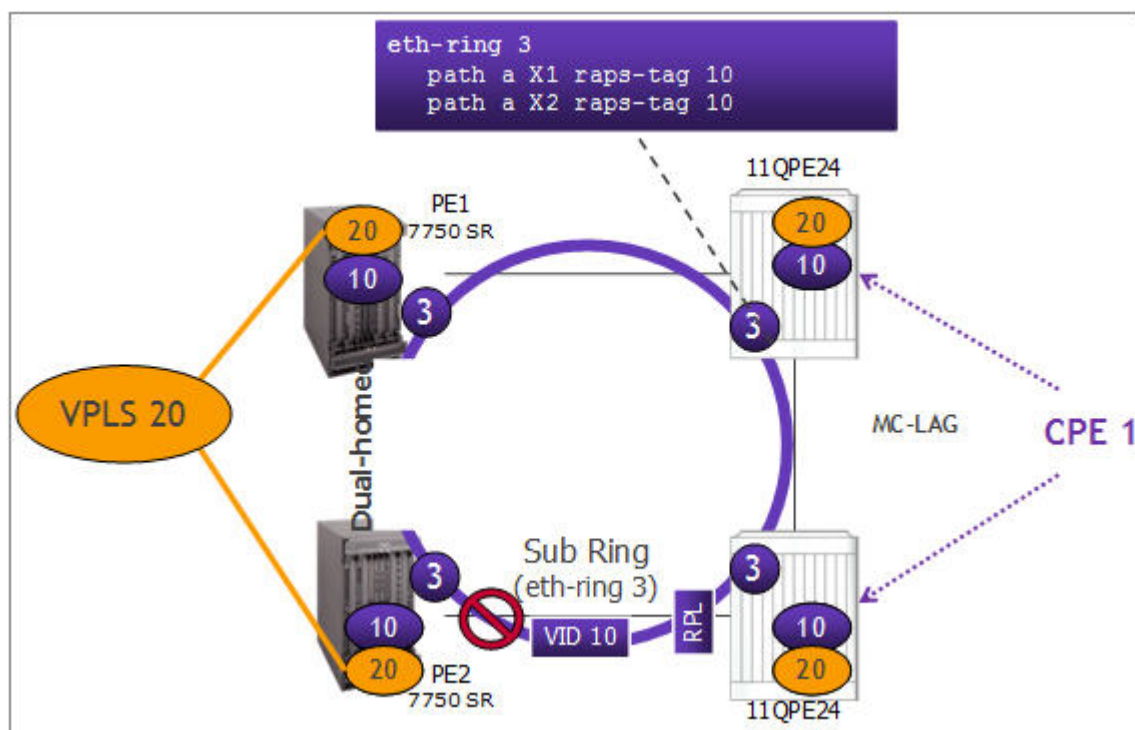


Figure 15-22 Dual Homed Sub-ring control

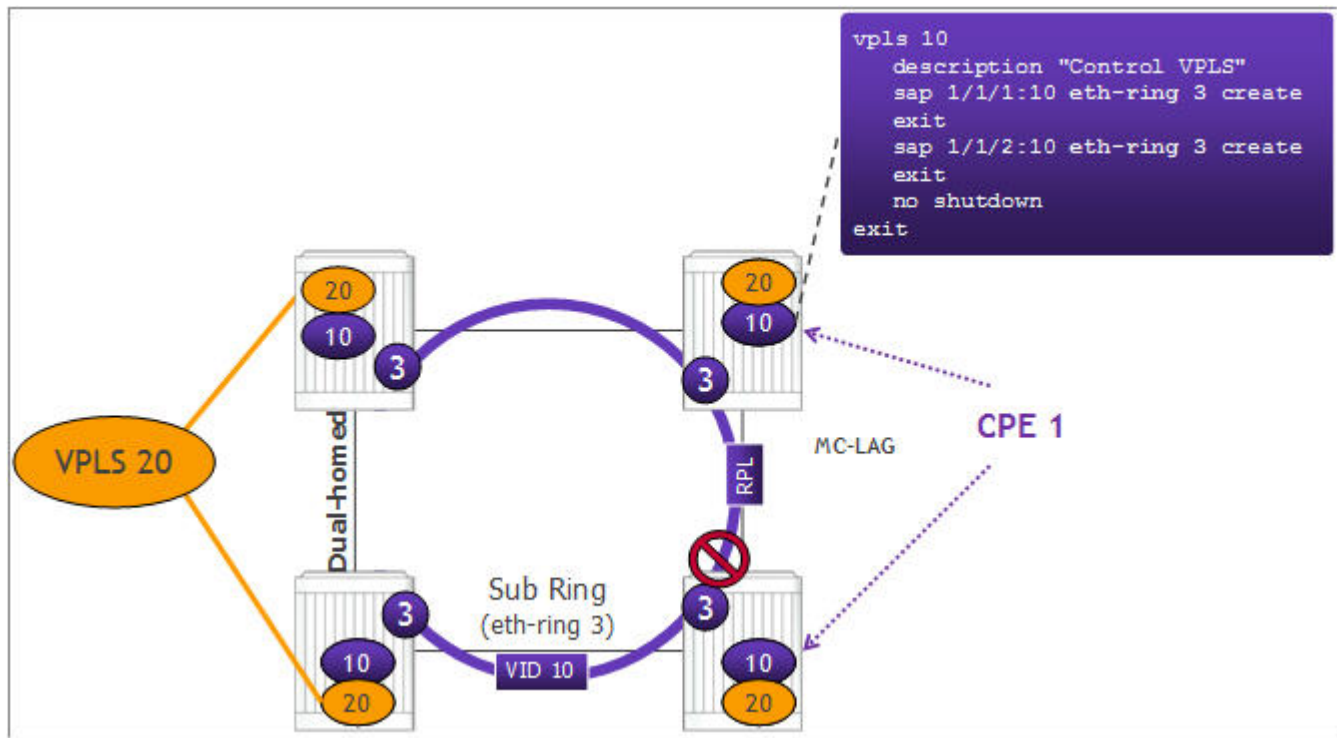
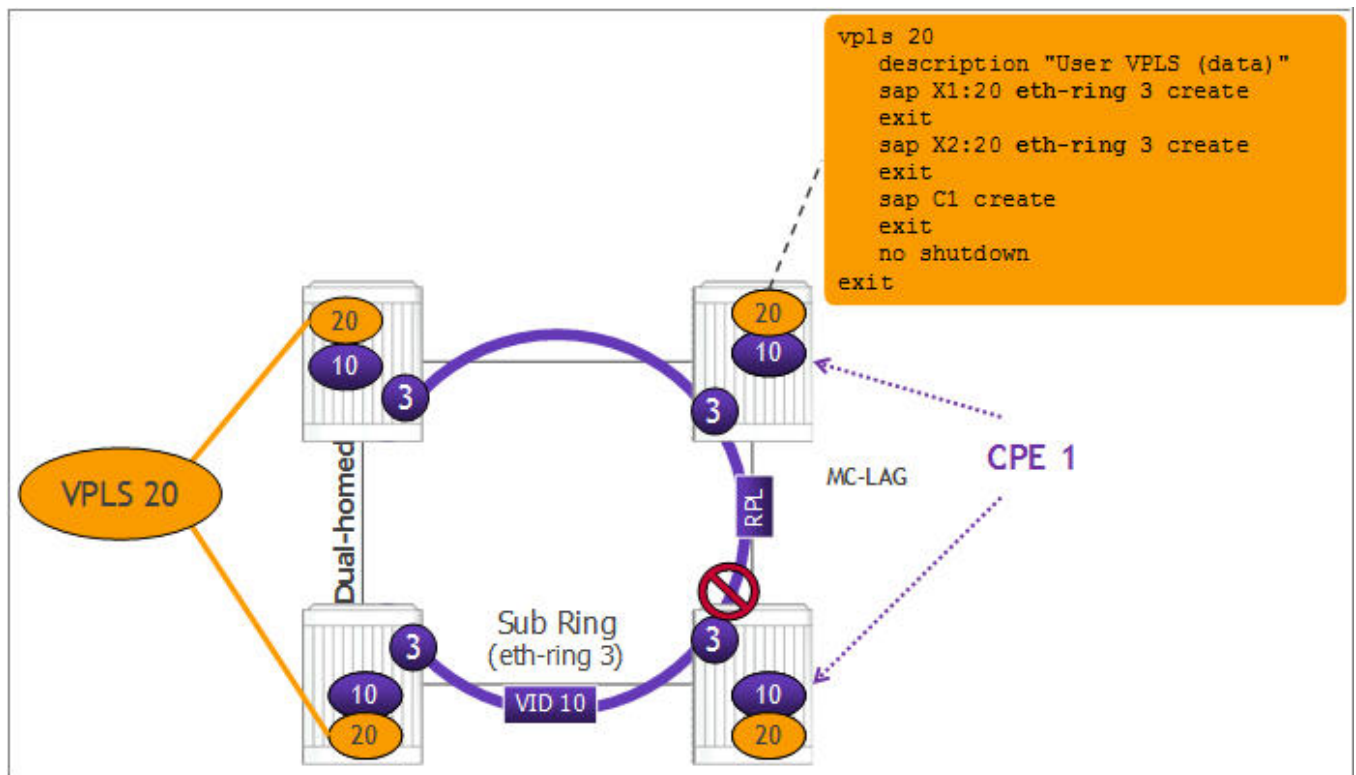
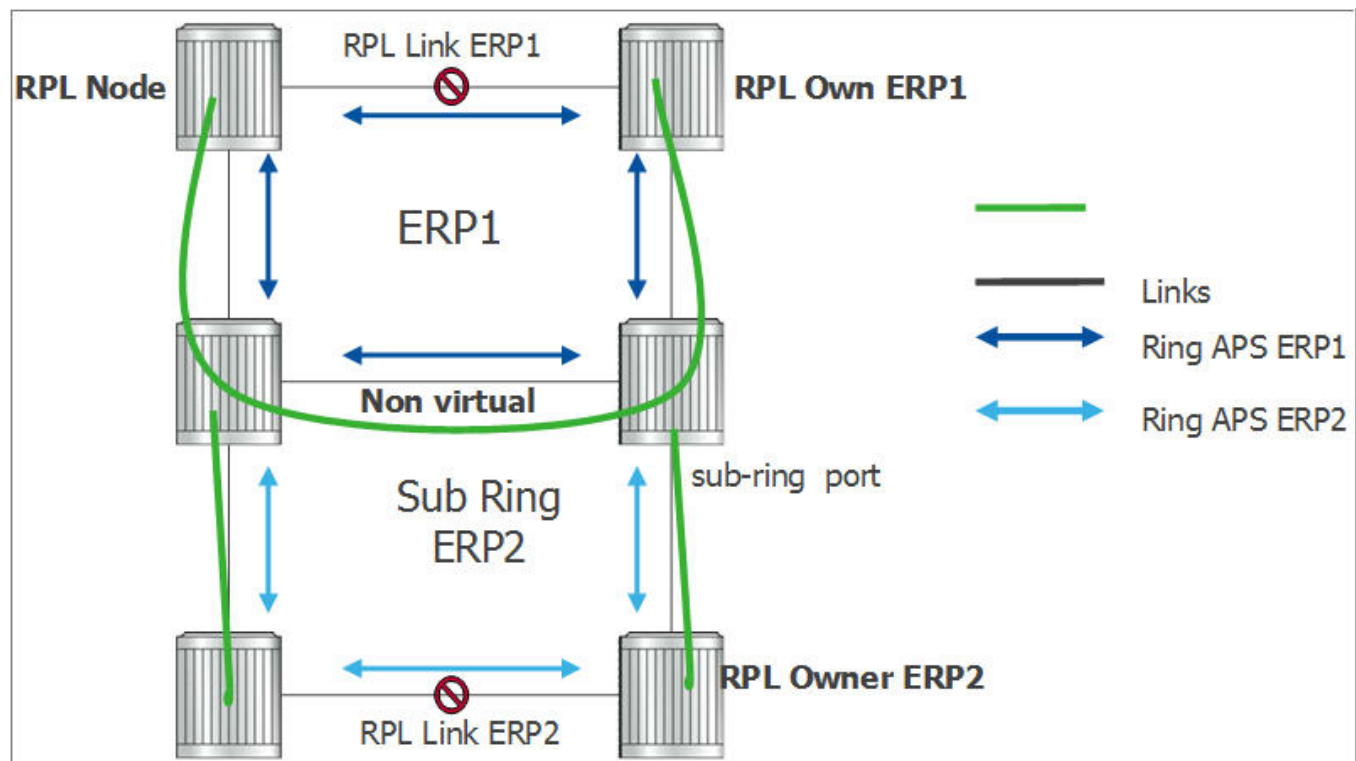


Figure 15-23 Data VPLS creation on Dual Homed Sub-ring**Major ring with virtual sub-ring**

The following [Figure 15-24, “Major ring with virtual sub-ring configuration”](#) (p. 15-38) illustrates a sample for this configuration.

Figure 15-24 Major ring with virtual sub-ring configuration



The following examples illustrate the Interconnecting nodes configuration.

Figure 15-25 Interconnecting Nodes: Ring Creation

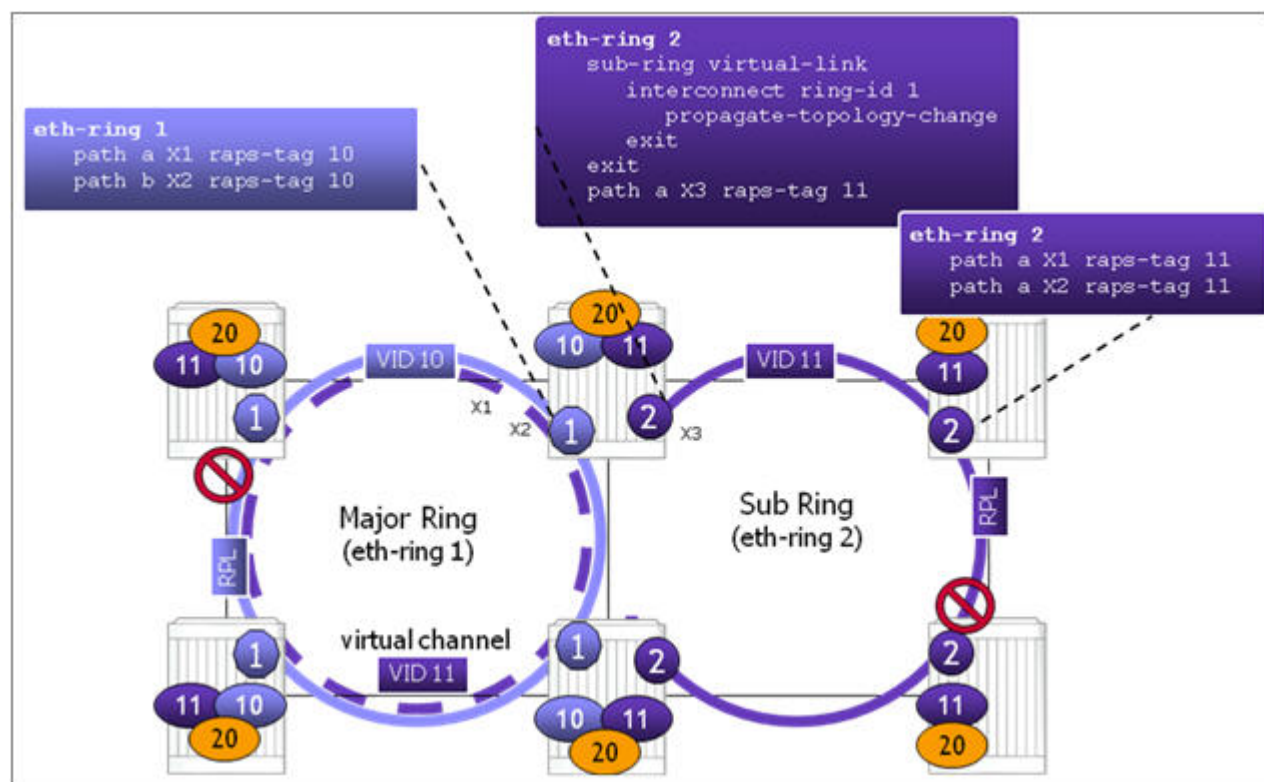


Figure 15-26 Interconnecting Nodes: Configuration Service (control and User data)

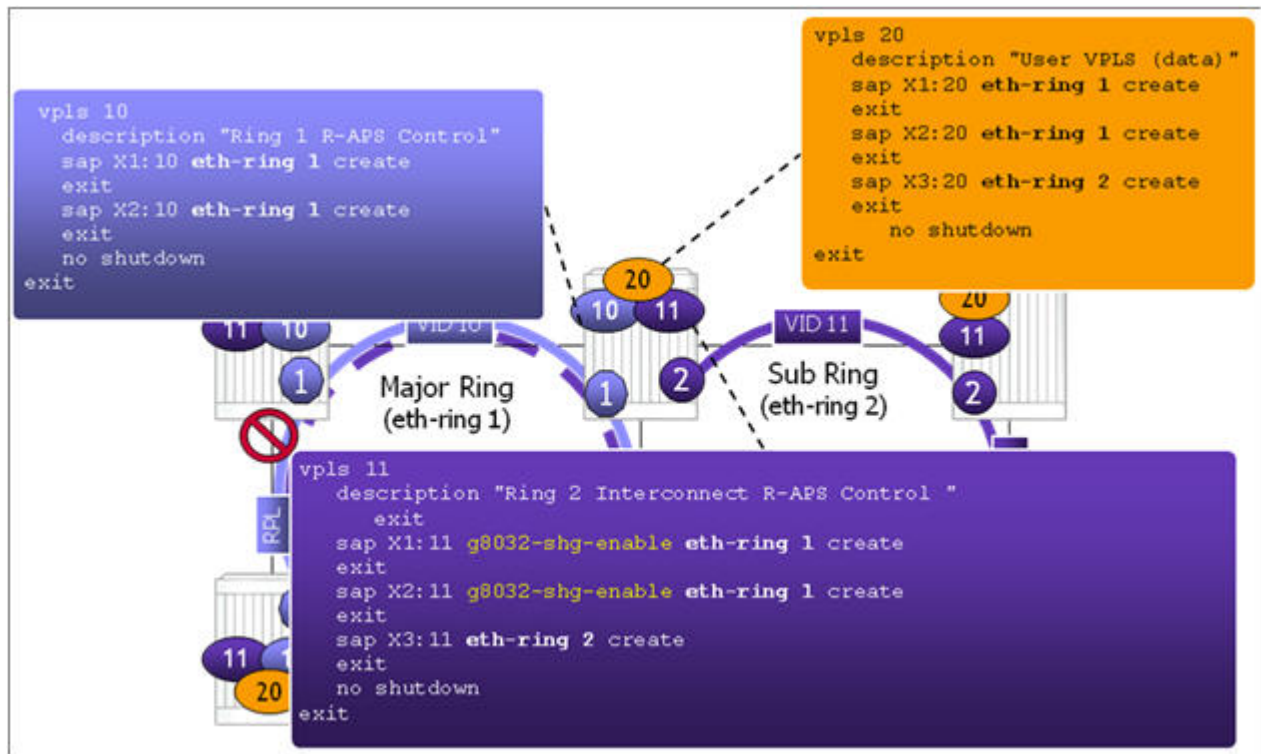


Figure 15-27 Major Ring: Configuration Service (control and User data)

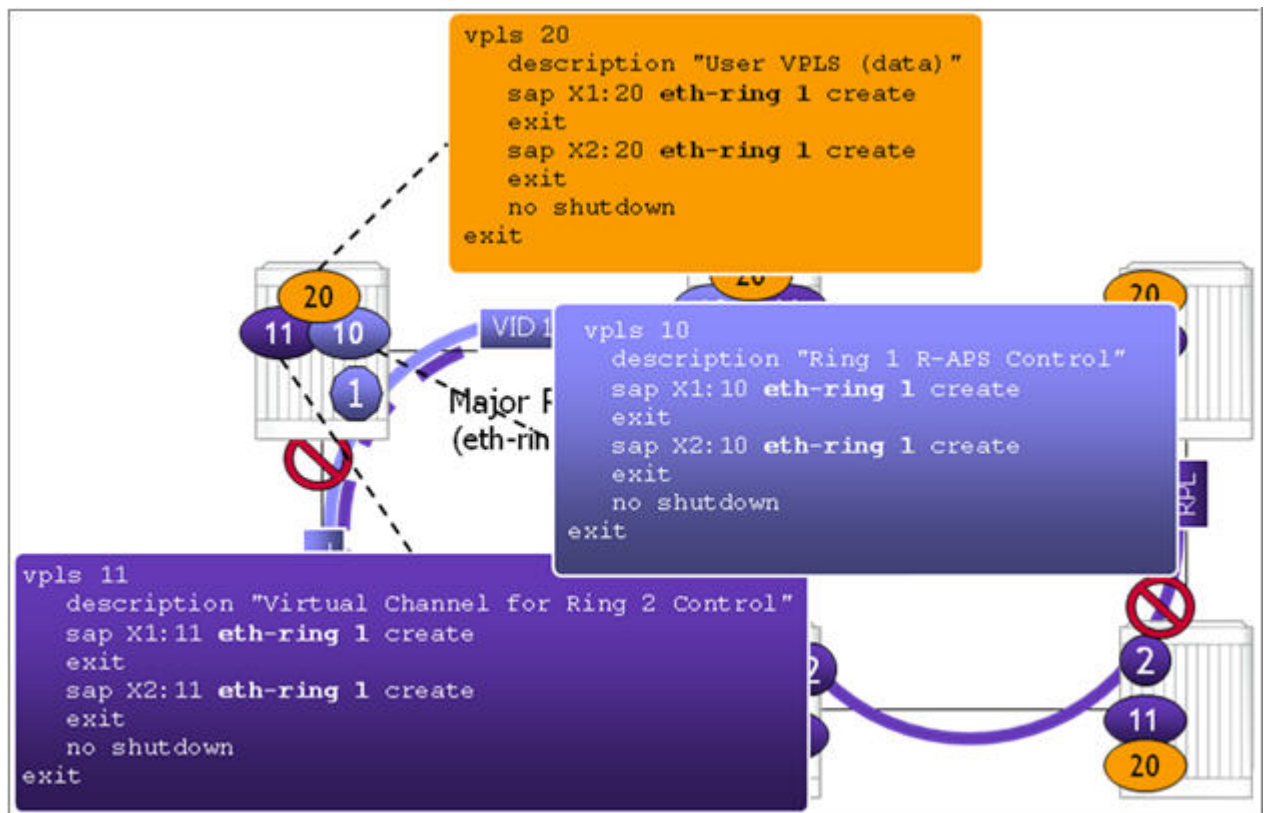
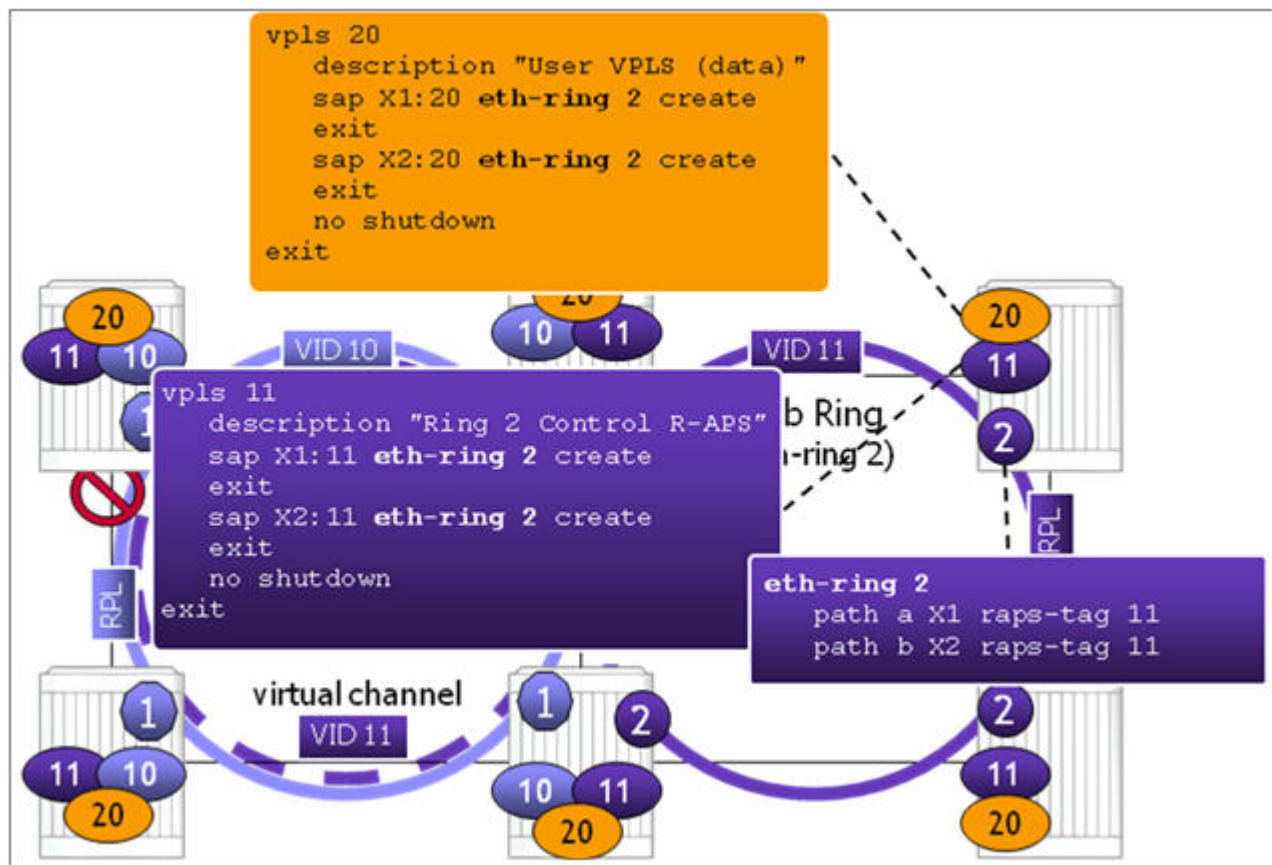


Figure 15-28 Sub-Ring Configuration Service (control and User data)

Multi-Chassis LAG (MC-LAG)

Multi-chassis LAG (MC-LAG) is a very powerful extension of the “regular” LAG and LAG sub-group concept that provides both node-level and card-level redundancy in addition to link-level redundancy. A CE running LAG in active/stand-by with LACP can be dual-homed to two SROS L2 packet cards, which can reside in the same or different shelves and MC-LAG will cover both link and card failure.

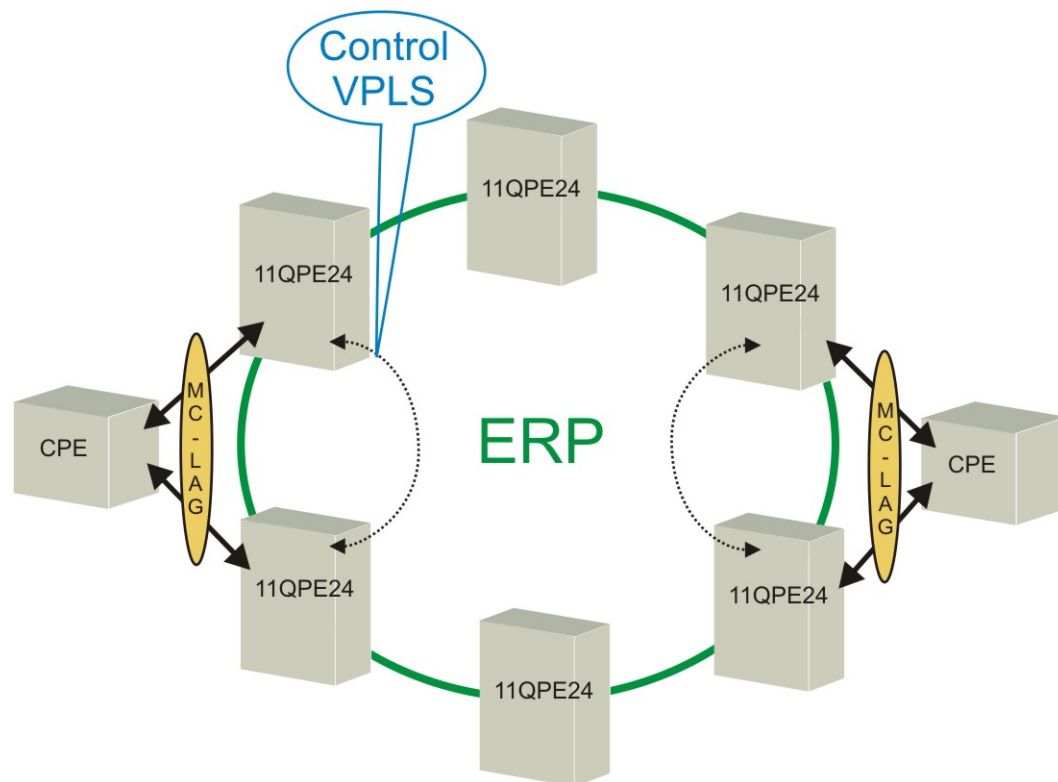
Typically, MC-LAG is deployed in a network-wide scenario providing redundant connection between different end points. The whole scenario is then built by a combination of different mechanisms (for example, MC-LAG and ERP to provide redundant connection in Layer 2.)

MC-LAGs are used for equipment protection of Ethernet services on UNIs, especially on 1 GbE handoffs. They can also be used on 10G UNI X ports. They cannot be used on ports running ERP or on NNI ports.

A dedicated MC-LAG control service needs to be set up between the paired cards, over which a specific protocol is run that makes the card pair look like a single LAG from the perspective of the CE.

The multi-chassis LAG protocol between the redundant-pair ensures a synchronized forwarding plane to and from the access node. It is used to synchronize the link state information between the redundant-pair nodes so that proper LACP messaging is provided to the access node from both redundant-pair nodes. To ensure SLAs and deterministic forwarding characteristics between the access and the redundant-pair node, multi-chassis LAG provides an active/standby operation towards/from the access node. LACP is used to manage the available LAG links active and standby states so that only links from one aggregation node are active at a time to and from the access node.

Figure 15-29 MC-LAG application



In order to ensure SLAs and deterministic forwarding characteristics between the access and the redundant-pair node, the multi-chassis LAG function provides an active/standby operation towards/from the access node. LACP is used to manage the available LAG links into active and standby states such that only links from one aggregation node are active at a time to/from the access node.

The 11QPE24 will support up to 20 MC-LAGs per card.

Each MC-LAG can have a maximum of four ports in an MC-LAG subgroup on each card.

The following illustrations show how MC-LAG can be used to provide protection.

Figure 15-30 MC-LAG card resiliency (different cards in a single node)

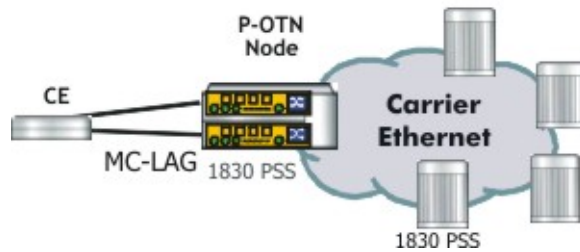


Figure 15-31 MC-LAG node resiliency (paired nodes)

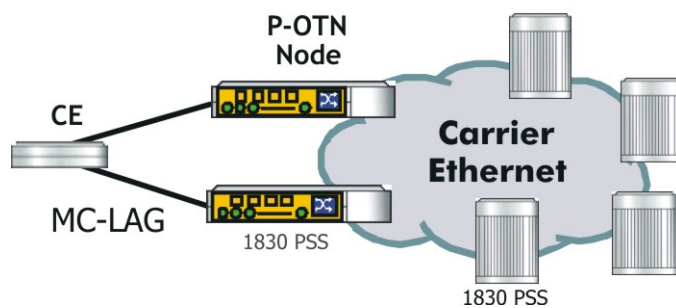


Figure 15-32 MC-LAG paired nodes with single router

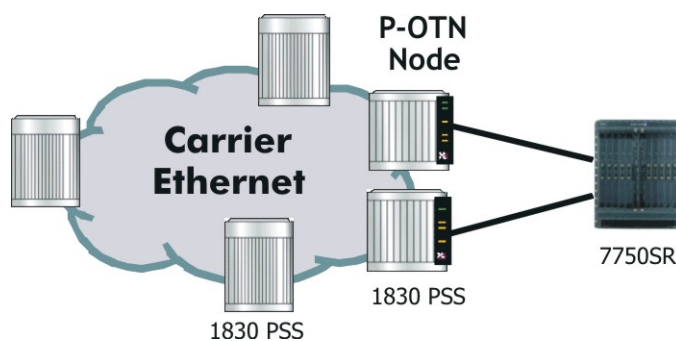
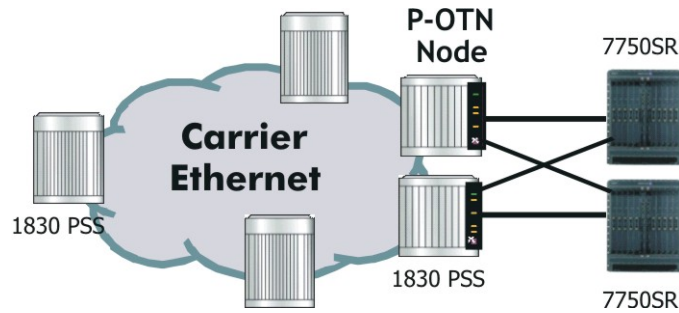


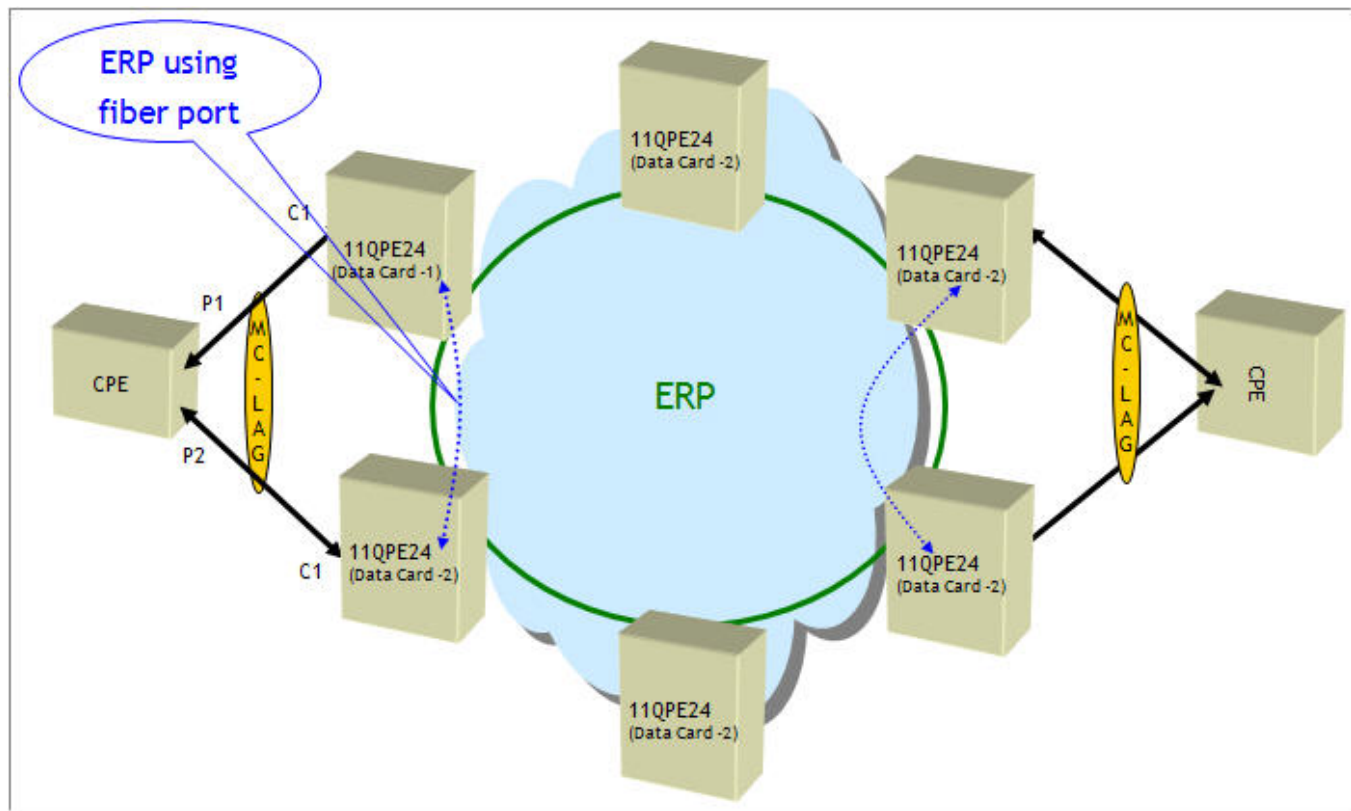
Figure 15-33 MC-LAG paired nodes with paired routers**LAG across cards through mate interface**

LAG across cards uses MC-LAG and provides 1+1 equipment protection when combined with ERP or MPLS-TP. Mate ports on adjacent cards provide the inter-card connectivity needed by MC-LAG control, without using faceplate ports and fibers. This in turn allows the support of more rings, for example.

Mate interfaces connecting 2 cards of a pair across the backplane are available on SROS L2 packet cards (except the 11QPE24), and in the 1830 PSS-4/8/16II/32 (but not 1830 PSS-16) shelves.

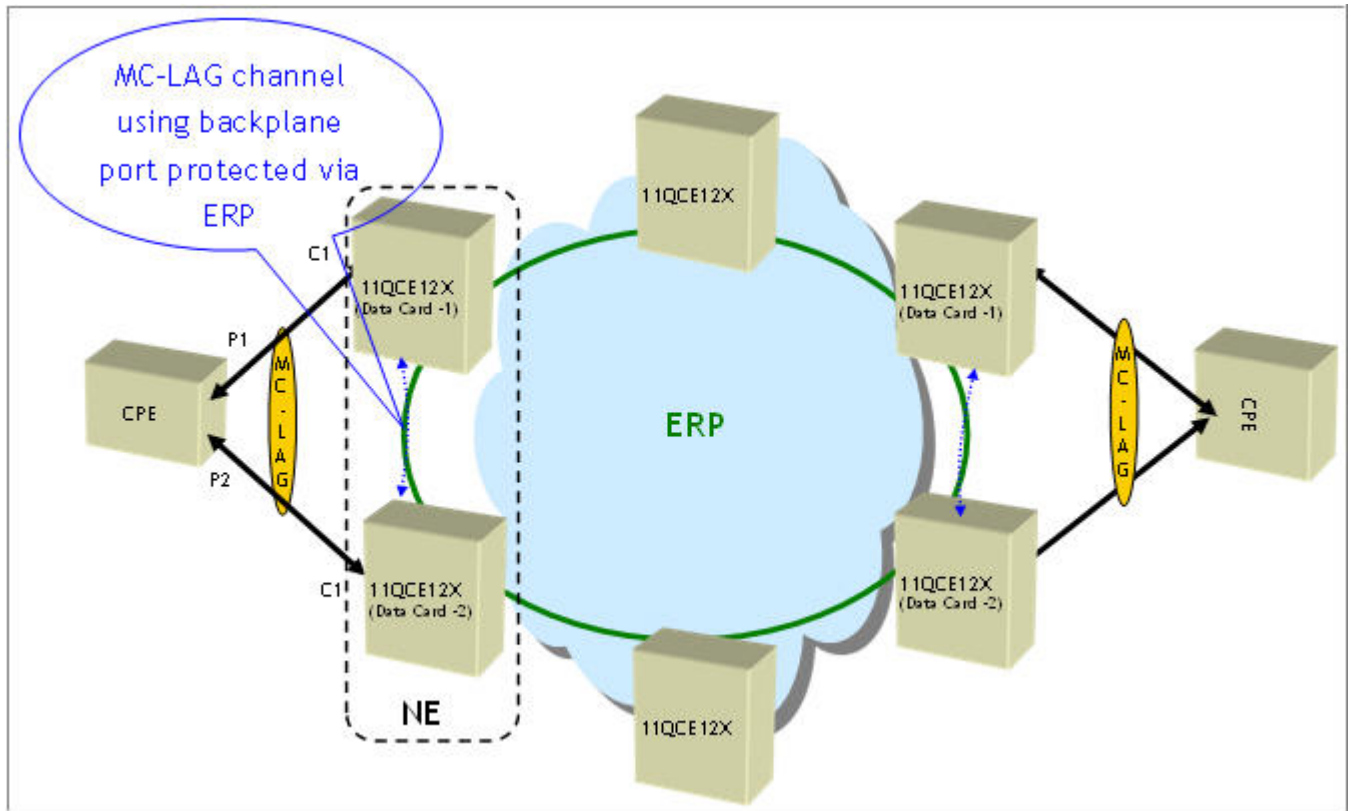
When not using mate ports between the cards, such as on 11QPE24s, [Figure 15-34, “MC-LAG current view” \(p. 15-46\)](#) shows the ring closure using faceplate ports and fibers.

Figure 15-34 MC-LAG current view

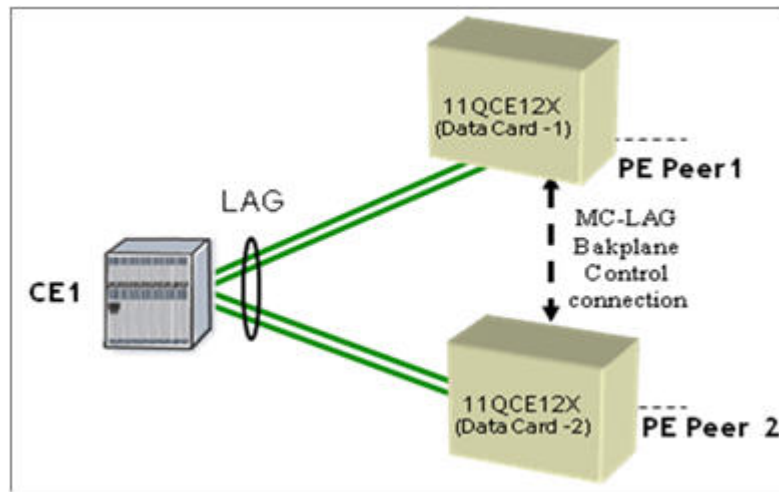


In Release 7.0, MC-LAG peer to peer control messages are carried on the backplane ports that carries traffic and is protected over ERP. In this set up user traffic, MC-LAG channel, and ERP R-APS channel are carried on the internal backplane ports configured similar to fiber ERP ports.

Figure 15-35 MC-LAG with ERP



To support MC-LAG across mate cards, backplane ports are provided on the 11OPE8 and 11QCE12X packs. Each pack has four backplane interface capable of supporting 4x10 GbE (XAUI) ports allowing a card pair to be used for equipment protection. The current MC-LAG and related ERP rules that apply for existing X ports also apply for the mate ports.

Figure 15-36 MC-LAG across mate cards

The backplane ports are only used as 4x10 GbE LAN (XAUI) ports. These ports are managed as any other 10 GbE ports (Ethernet) (no OTU2 functionality), except that there is no associated XFP or SFP+ connected.

L2 Smart SFP & Smart cEDD remote management

The L2 OAM Smart SFPs and Smart cEDD, collectively called Smart devices or Remote Managed Devices (RMD), are remotely managed from the SROS L2 packet cards which integrates a Proxy Remote Management Agent (RMA). A large number of parameters can be configured and information, status, alarms can be retrieved from the Smart devices.

The following hardware is available and used exclusively in conjunction with SROS L2 packet cards:

- **L2 OAM Smart SFP - CFM or EFM OAM version** - L2 OAM Smart SFP is a pioneering concept of miniaturizing an Ethernet NID into an SFP that plugs directly into the Customer Edge (CE) equipment, but that is owned by the Ethernet Service Provider and remotely managed from the 1830 PSS. Smart SFPs provide a significant power (they are passive), footprint, and cost reduction but also massively improve the reliability of the last mile with their impressive MTBF compared to a stand-alone

NID. They exist in different versions: a family of APNs supporting IEEE 802.3ag EFM OAM, another supporting IEEE 802.1ag CFM OAM. In each family different reaches and optical types are provided: duplex 10 km and 80 km, bidirectional 20 km, and 40 km (uplink and downlink). **Note:** The SFP used on the 11QPE24 and 11QCE12X side is a regular one.

- **Smart cEDD** - A very compact, low-cost, low-power, simple to operate 1 GbE demarcation device that implements IEEE 802.1aj Two Port MAC Relay (TPMR) and IEEE 802.1ag CFM at link-level. It is used for simple demarcation applications not requiring the features and prices of a traditional full-featured Ethernet NID, but when the Smart SFP is not an option either because the CE does not accept third-party SFP or because customer preference or regulation imposes a physical demarcation device. The cEDD is equipped with a DC power feed but can be offered with AC/DC power converter.

For more information on this topic, see [“Smart device OAM demarcation and management”](#) (p. 15-92).

QoS L3/L4 classification

Note: In Release 7.0.1, the 11OPE8 card supports the following features in addition to 11QPE24 and 11QCE12X which already supports them.

L3/L4 QoS match criteria classification are supported on SAP ingress policies. These new classifications are also used with ingress meters for policing and mapping into forwarding class to provide a complete QoS solution.

Classification is enhanced by the following additions:

- IP Match criteria
- DiffServ Code Point DSCP (no change from Release 6.0)
- IP source and mask
- IP destination and mask
- IP protocol
- TCP/UDP source port or port range
- TCP/UDP destination or port range

IPv6 Match criteria

- DiffServ Code Point DSCP
- IPv6 128-bit source and mask
- IPv6 128-bit destination and mask
- IP protocol/next-header
- TCP/UDP source port or port range
- TCP/UDP destination or port range

MAC based matching

- IEEE 802.1p value/mask
- Source MAC address/mask
- Destination MAC address/mask
- EtherType value

Port loopback with MAC swapping

The system enables PHY/MAC loopback on a specified port when the Port loopback command with MAC swap is enabled. All the packets are sent out of the port configured for loopback and received back by the system. On ingress to the system after the loopback, the node swaps the MAC addresses for the specified SAP and the service. It only processes packets that match the specified source MAC address and destination MAC address, and drops the packets that do not match. It processes these packets as per the service configuration for the SAP.

Note: To implement this feature, the system needs one unused port "no-service-ports" to be configured as a loopback-no-svc-port. On the 11QCE12X port, C23 and C24 are unused internal ports and are used for loopback-no-svc-port. A physical face plate port can also be used.

This feature affects all services provisioned on the port.

Note: Before enabling this feature, all layer 2 control protocols should be turned off on the port and its peer to prevent errors such as protocol flaps due to timeout. When the loop back is enabled, ensure that Ethernet parameters such as speed, duplex, auto-negotiation and so on are not modified.

Frame based accounting policy

This feature when enabled, allow QoS policies to account for the Ethernet frame overhead (for example, it accounts for the IFG (inter-frame gap) and the preamble). Typically, the IFG and preamble constitutes about $12 + 8 = 20$ bytes. The overhead for Ethernet ports uses this value. A configurable CLI command enables accounting of the frame overhead at ingress or egress. When disabled, the queue rates and egress-rate do not account for the Ethernet frame overhead. By default frame-based accounting is disabled for both ingress and egress.

MAC move

MAC move protects against undetected loops in a VPLS topology as well as the presence of duplicate MACs in a VPLS service.

MAC move is supported on the following cards:

- 11OPE8
- 11QCE12X
- 11QPE24

If there are two clients in the VPLS having the same MAC address, the VPLS will experience a high re-learn rate for the MAC. When MAC move is enabled, the system will shut down the SAP and create an event (SAP-MAC-MOVE-EXCEEDED) when the threshold is exceeded.

IPv6 TC/DSCP ingress classification

Note: In Release 7.0.1, the 11OPE8 card supports the following features.

This release adds the IPv6 DSCP classification criteria option in the QoS SAP Ingress policy, completing the classification criteria supported in the previous release and meeting the requirements of MEF 10.2 for the CoS ID EVC Service attribute.

Starting in Release 6.0, IPv6 QoS criteria-based classification SAP ingress policies can be used to select the appropriate ingress meters and corresponding forwarding class for matched traffic. The policy entries allow classification on IPv6 DiffServ code point.

The IPv4/IPv6 and MAC match criteria can be very basic or quite detailed. IPv4/IPv6 and MAC match criteria are constructed from policy entries. An entry is identified by a unique, numerical entry ID. A single entry cannot contain more than one match value for each match criteria. Each match entry has an action which specifies: the forwarding class of packets that match the entry. The entries are evaluated in numerical order based on the entry ID from the lowest to highest ID value. The first entry that matches all match criteria has its action performed

Color-aware policing (E-NNI)

The MEF Bandwidth Profile algorithm includes a Color Mode (CM) parameter. For this color-aware mode parameter, each service frame is already associated with a color; that color is taken into account in determining the level of compliance by the IBWP algorithm. In color-blind mode, the color (if any) already associated with each service frame is ignored by the IBWP algorithm.

Color-aware policing for MEF E-NNI is supported indirectly by configuring a network QoS policy with meters and policers on uplink (NNI) ports with Q-in-Q encapsulation.

Weighted Random Early Detection (WRED)

Pro-active Queue Congestion Management

Proactive queue management is implemented to signal congestion before the queue is full and provides considerable performance advantages over a traditional tail-drop approach which drops any packet arriving on a full queue. It is a packet drop policy that avoids congestion by dropping packets proactively to signal congestion to traffic sources with end-to-end adaptive feedback control (that is, TCP Sessions).

Random Early Detection (RED) attempts to preemptively drop packets before congestion occurs. Dropping is done based on a calculation of probability. This is intended to avert “global” TCP synchronization (simultaneous dropping to minimum window size by multiple TCP sessions as a result of significant packet drops, that is, acks for multiple sessions) during congestion.

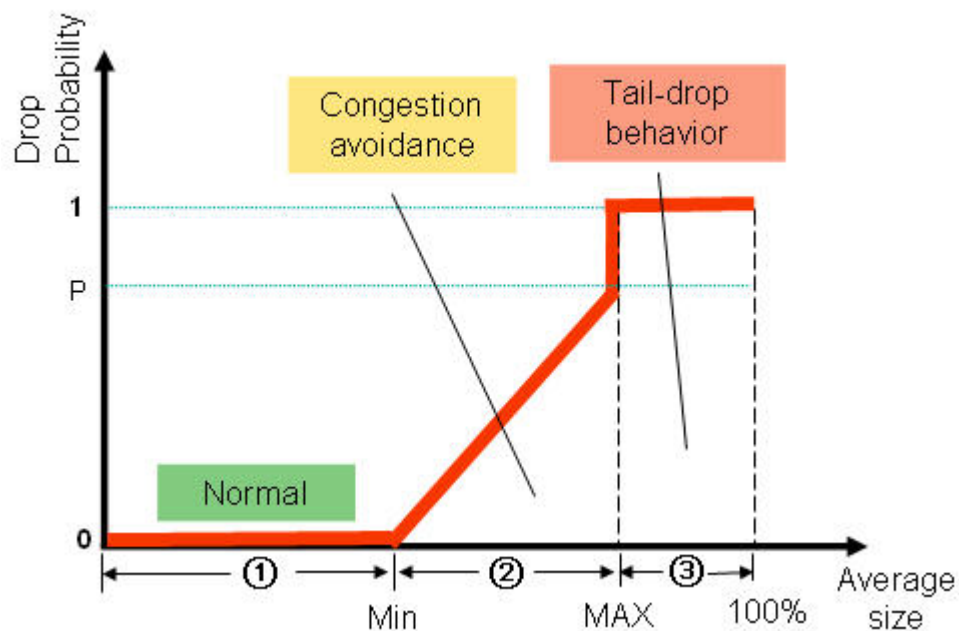
Typically, RED provides resource management on a single queue associated with an egress port. Weighted Random Early Detection (WRED) is the same except that it uses separate profiles for each FC and packet priority/color. Additionally, a separate profile can be defined for non-TCP traffic so that a more aggressive drop probability profile (slope) can be employed for this traffic, preventing non-TCP traffic from consuming resources while TCP traffic is being “throttled” by packet loss.

WRED Slope policies are supported on all ports (access and uplink) egress queues. Slope policies are defined for In-profile TCP high-slope (green) packet, out-of-profile TCP low-slope (yellow) packets, and non-TCP slope packets.

Random Early Detection (RED)

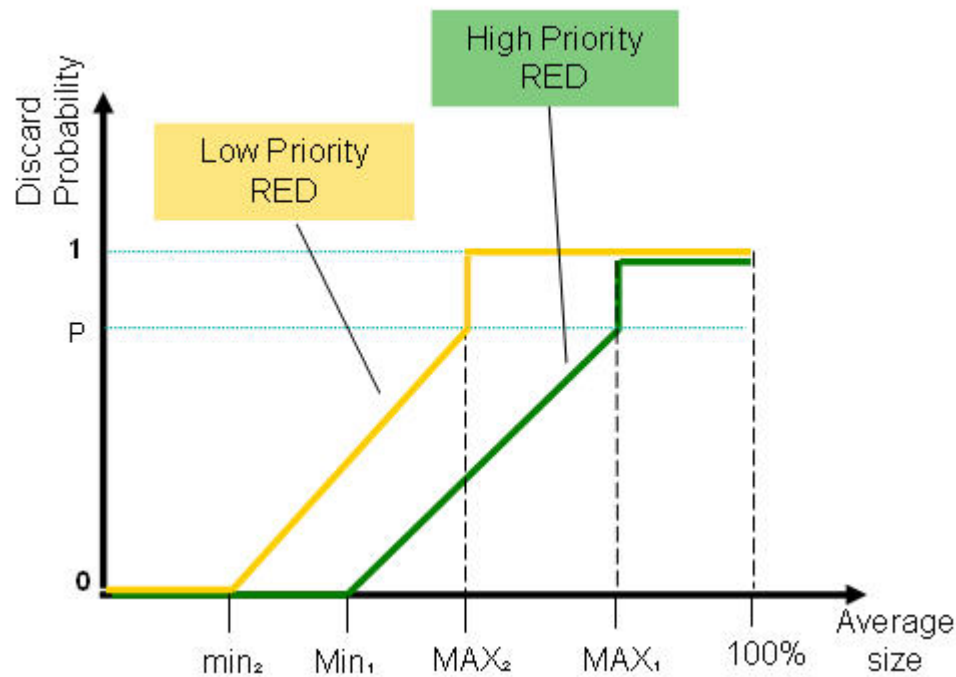
Instead of waiting until the queue is completely filled up, RED starts dropping packets with a non-zero drop probability after the average queue size exceeds a certain minimum threshold. Packet drop probability is a linear function of the average queue size. A drop probability ensures that RED randomly drops packets from only a few flows, avoiding global synchronization.

For average queue size up to a lower threshold, minimum, packet-drop action is not activated (drop probability is zero). When the average queue size is above the minimum threshold, RED starts dropping packets. The packet drop rate increases linearly as the average queue size increases, until it reaches the maximum threshold. When the average queue size is above the maximum threshold, all packets are dropped.

Figure 15-37 Random Early Detection (RED)**Weighted Random Early Detection (WRED)**

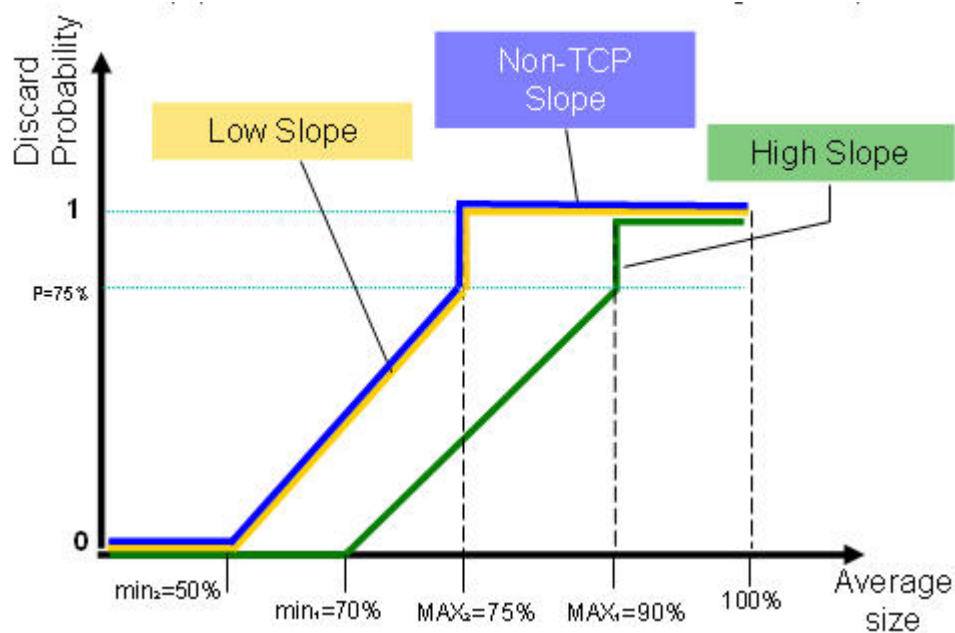
In Release 6.0, Weighted Random Early Detection (WRED) introduces grades of service among packets based on a packet's drop probability and allows selective RED parameters based on packet's drop precedence. As a result, WRED drops more aggressively for low priority/out-of-profile packets and less aggressively for high priority/in-profile packets.

As shown in the illustration below, the congestion handler selects one of two curves for a single queue based on packet priority/color. High priority/in-profile packets are subject to discard action with increasing probability in case the occupancy is between the Min and MAX threshold. Otherwise the discard function rises to 1. Low priority/out-of-profile packets are subject to a more aggressive curve in which frame drops begin at a lower average occupancy level, the Min, increasing rapidly to 1 at MAX.

Figure 15-38 Weighted Random Early Detection (WRED)**WRED slope policies**

Each shared buffer pool is associated with a default slope policy based on the port/queue. The default slope-policy is DISABLE and it does not have an effect on traffic. The user must create its own policy and enable it for specific queues. In Release 6.0, WRED Slope policies are supported on all ports (access and uplink) egress queues. Slope policies are defined for In-profile TCP high-slope (green) packet, out-of-profile TCP low-slope (yellow) packets, and non-TCP slope packets. In the following figure, the default values are presented.

The congestion handler selects one of three curves for a single queue based on different traffic types and drop precedence. The non-TCP slope manages access to the shared portion of the buffer pool for non TCP packets destined for a given queue. The out-of-profile TCP low-slope manages access to the shared portion of the buffer pool for out-of-profile/yellow packets destined for a given queue. The In-profile TCP high-slope, manages access to the shared portion of the buffer pool for in-profile/green packets destined for a given queue. In addition, a configurable Time Averaging Factor is provided which allows control over how the average queue size is calculated.

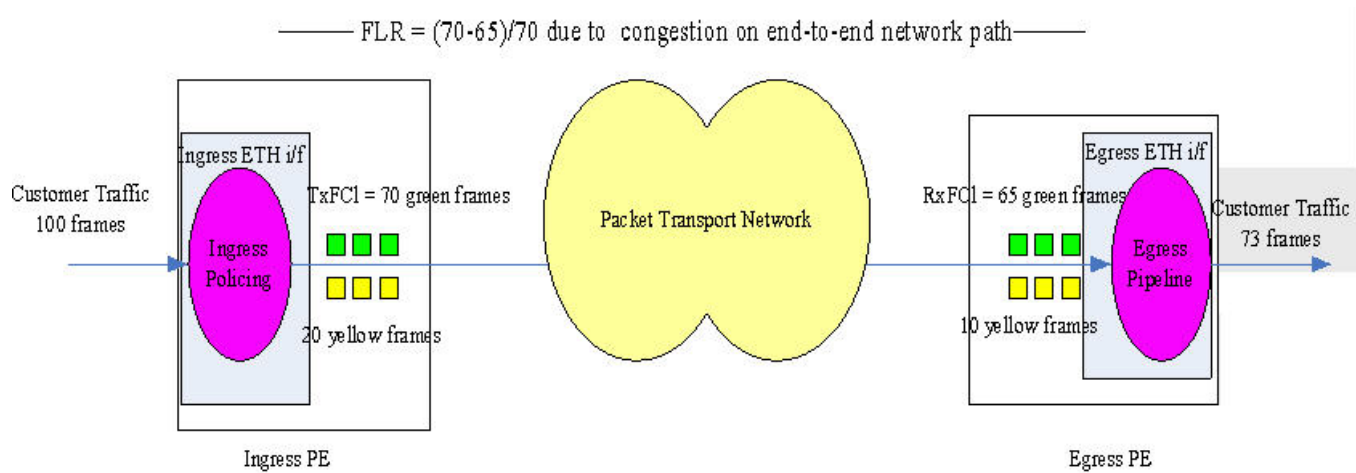
Figure 15-39 WRED slope policies**Ethernet Loss measurement (ETH-LM)**

The purpose of ETH-LM is to count the number of lost service frames which are not successfully delivered to the specified destinations, for one EVC due to the following reasons

- Dropped frame due to network congestion or wrong behaviors
- Errored frames (Corrupted header or errored payload)
- Delivered to other unpermitted destinations

In a point-to-point ETH connection, the number of lost frames on one EVC shall be the difference between TxFCI counter and RxFCI counter which are defined below:

1. TxFCI: the number of service frames arriving at the ingress ETH flow point which shall be delivered to egress ETH flow point and whose level of ingress bandwidth profile compliance is determined to be green
2. RxFCI: the number of service frames within the same traffic flow specified above delivered at the egress ETH flow point.

Figure 15-40 Ethernet frame loss concept**ITU-T Y.1731 LM/SLM and DM pro-active**

Note: This feature is supported on 11DPE12A and SROS L2 packet cards except for LM, which is only supported on 11DPE12A.

ITU-T Y.1731 single-ended ETH-SLM and ETH-DM Service OAM functions implemented in Release 5.1 were on-demand. In this release they are extended to pro-active, with continuous transmission of associated OAM PDUs at regular intervals. They are used typically on an Up MEP for Service OAM, for both point-to-point and multipoint services. This provides compliance to the (mandatory) PM-1 solution in MEF 35 “Service OAM Performance Monitoring Implementation Agreement”.

Each pro-active OAM test is configured similarly to on-demand tests (with same configurable options) but is also associated to a Level 2 PMON policy. The Level 2 PMON policy defines the bin type and TCAs. The pro-active test starts when a SLM or DM PMON policy is attached. Upon pro-active test deletion, the associated PMON bins are deleted and the TCAs cleared. The configured MEP and CoS as per ITU-T Y.1731 SLA parameters in MEF 10.2 are measured per CoS ID. The frame loss and delay behaviors are different in different queues.

Scalability of pro-active ITU-T Y.1731 SLM/DM configuration:

- 32 simultaneous pro-active tests per type (SLM or DM) per card. Test can be freely arranged over any MEP and across CoS (that is, FC) on an MEP and specifically for 11DPE12A and SROS L2 packet cards, 100 simultaneous pro-active tests per type (LM/SLM or DM) per card.
- On-demand and proactive tests are exclusive on a (MEP, CoS)
- Up to eight policies per PMON type

Pro-active ITU-T Y.1731 SLM

Synthetic LM as defined in ITU-T Y.1731 §8.4 uses synthetic frames (SLM) as opposed to actual service frames as does LMM. SLM works for point-to-point and multipoint. SLM is a single ended-measurement: Initiator/Source MEP sends SLM, and the responder MEP replies with SLR. MEP

MEP maintains the following counters:

- TxFCf: count of SLM sent towards the peer MEP (inserted in SLM PDU) – initiator MEP
- TxFCb: count of SLR sent towards the peer MEP (inserted in SLR PDU) – responder MEP
- RxFCI: count of synthetic frames received from the peer MEP – initiator MEP

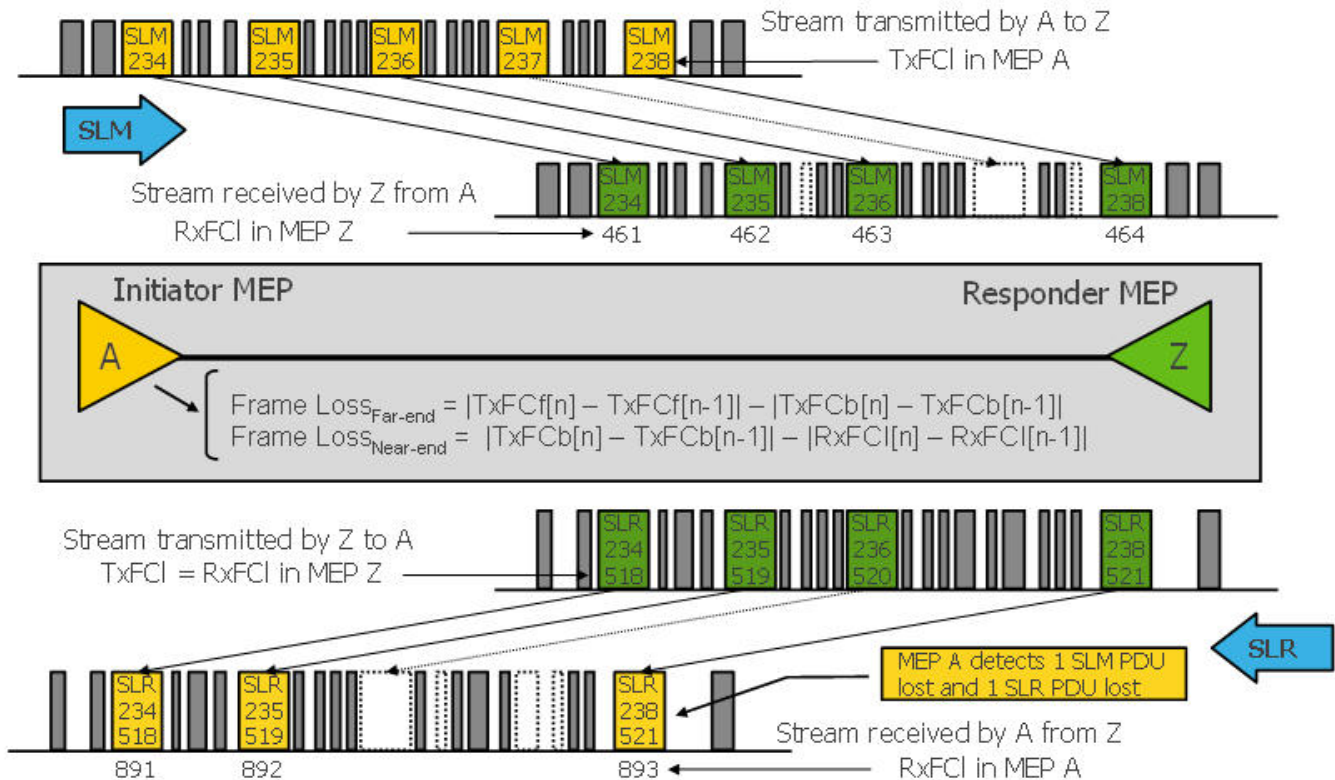
The count comparison determines the frame loss in each direction (near-end/far-end). With pro-active SLM, these measurements are made continuously. They are used to measure the Frame Loss Ratio (FLR) as follows:

- Far-end FLR = $(\Delta\text{TxFCf} - \Delta\text{TxFCb})/\Delta\text{TxFCf}$
- Near-end FLR = $(\Delta\text{TxFCb} - \Delta\text{RxFCI})/\Delta\text{TxFCb}$

Figure 15-41 Pro-active ITU-T Y.1731 SLM

Pro-active ITU-T Y.1731 ETH-SLM

How it works



Pro-active ITU-T Y.1731 DM

Pro-active frame Delay Measurement (DM) is based on 2-way DMM/DMR as defined in ITU-T Y.1731 § 8.2.2., as follows:

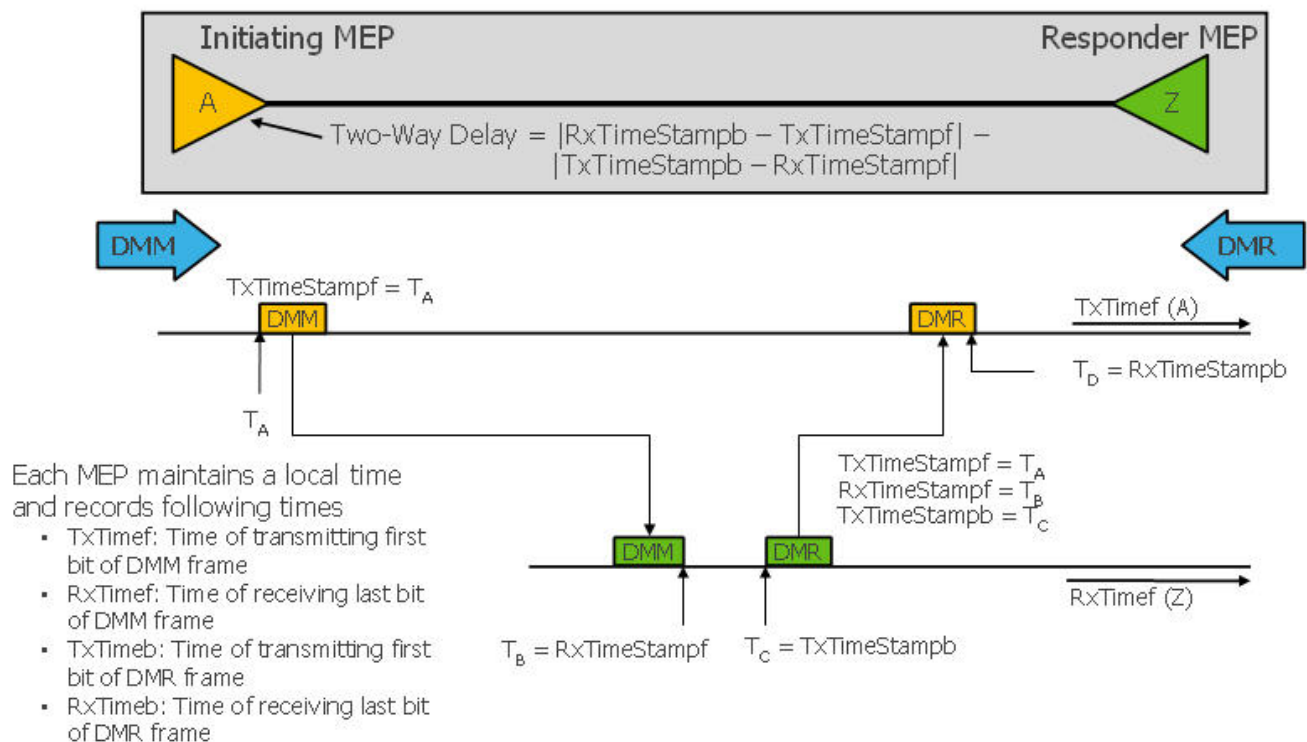
- Measures round-trip frame delay and 1-way frame delay variation between a pair of MEPs in a MEG
- Measures delay on the forward and return path between initiator and responder
- Single-ended measurement: initiator MEP sends DMM, responder MEP replies with DMR
- Round-trip delay does not require synchronized clocks on both sides
- Each MEP maintains local timestamps and exchanges DMM or DMR at certain configurable intervals with the peer MEP

The frame delay is calculated from the comparison of timestamps contained in DMM and DMRs, in each direction (near-end/far-end). The delay variation is computed from the differences of multiple delay measurements. With pro-active DM, these measurements are made repetitively.

Figure 15-42 Pro-active ITU-T Y.1731 DM

Pro-active ITU-T Y.1731 ETH-DM

How it works



ITU-T G.7710 PM with 15/24 hrs binning and thresholding

Note: This feature is supported on 11DPE12A and 11QPE24. In Release 7.0.1, the 11OPE8 card also supports the following features.

The traditional methods for Performance Monitoring defined by ETSI and ITU-T recommendations for SDH, SONET, OTN transport networks are now available for packet counters, with accumulation in 15-min and 24-hrs bins, bin archiving and optional Threshold Crossing Alerts (TCA). PMON binning applies to the following counter entities:

- Port (for both access [UNI] or uplink [NNI])
- SAPs (UNI)
- egress queues
- pro-active OAM tests

PMON is activated by creating PMON policies and associating them to the monitored entities. Up to 33 x 15-min bins, 8 x 1-day bins are provided, with 15-min TCA values and 1-day TCA values (applicable to certain counters only). The PM binning process starts as soon as a PMON policy is assigned to an entity. The binning process is stopped once the PMON policy is explicitly removed from the entity. The TR / 'Transient condition method' of G.7710 is supported for TCAs.

100ms period for ITU-T Y.1731 pro-active SLM and FLR accuracy improvement

Since release 5.1, ETH-SLM (Ethernet Synthetic Loss Measurement Function) defined in ITU-T Y.1731 and MEF17/35 is available on Up MEPs to measure frame-loss of an Ethernet service (EVC). Pro-active ETH-SLM was added in R6.0 with associated FLR SLA performance monitoring counters. This OAM function uses OAM PDUs called SLM (transmitted by Source MEP) and SLR (replied by Destination MEP). At the source MEP, the SLM PDU transmission period is configurable as per MEF35 [R76]. Periods supported are 1s (default) or 10s. SLM frame size is also configurable, compliant to MEF35 [R78].

Starting in R7.0.2/7.0.3, SLM frame rate is improved with the option for SLM PDU transmission period of 100ms. Configurable range is now {100 ms, 1 sec, 10 sec}. This allows improving the accuracy of FLR measured via SLM and fully complies with MEF35 [R77]. **Note:** The default remains 1s, compliant with MEF35 [D30], keeping same default on all cards and avoid upgrade problems.

This feature is implemented on 11OPE8 and 11QCE12X.

ETH-DM frame size configuration

Since release 5.1, ETH-DM (Ethernet Delay Measurement Function) defined in ITU-T Y.1731 and MEF17/35 is available on Up MEPs to measure two-way frame delay and one-way frame delay variation of an Ethernet service (EVC). Pro-active ETH-DM was added in R6.0 with associated FD/FDV SLA performance monitoring counters. This OAM function uses OAM PDUs called DMM (transmitted by Source MEP) and DMR (replied by Destination MEP). The DMM PDU transmission period is configurable as per MEF35 [R61]. Periods supported are 1s (default) or 10s.

Starting in R7.0.2/7.0.3, the option to configure the DMM frame size is supported in order to measure latency for different frame sizes. The DMM frame size is now configurable up to the 9.6k bytes (which corresponds to the MTU), compliant with MEF 35 [R63], [R64] and [D23]. This is done by configuring the "size", i.e. size of the data portion of the data TLV added to the frame.

This feature is implemented on SROS L2 packet cards 11QPE24, 11OPE8 and 11QCE12X.

ITU-T Y.1731/MEF 35 SLA counters for LM, SLM, and DM

Note: This feature is supported on 11DPE12A and SROS L2 packet cards except for LM, which is only supported on 11DPE12A.

The PM counters on 11DPE12A are listed in [Table 15-5, “PM Counters defined for pro-active DM on 11DPE12A” \(p. 15-63\)](#) up to [Table 15-5, “PM Counters defined for pro-active DM on 11DPE12A” \(p. 15-63\)](#).

The results of the Y.1731 pro-active SLM and DM measurements are accumulated in PM counters per Service and CoS as defined in MEF 35, stored in 15-min and 24-hr bins with optional TCA. These counters are used for Service SLA Monitoring, to verify conformance to Performance Objectives as specified in MEF 10.2.

The following table lists the MEF 35 PM counters for SLM. FLR is expressed uni-directionally. MEF 10.2 EVC-related performance service attributes are uni-directional. Average and extreme FLR in the measurement interval are relevant for SLA. TCA is only needed for average and maximum for SLA verification.

Table 15-1 PM Counters defined for pro-active SLM

PM Counters	Counter Acronym	TCA
Minimum Near-End FLR	mN_FLR	No
Average Near-End FLR	aN_FLR	Yes
Maximum Near-End FLR	xN_FLR	Yes
Minimum Far-End FLR	mF_FLR	No
Average Far-End FLR	aF_FLR	Yes
Maximum Far-End FLR	xF_FLR	Yes

The following table lists the MEF 35 PM counters for DM. Only average and maximum FD/FDV are relevant for SLA verification and need a TCA

Table 15-2 PM Counters defined for pro-active DM

PM Counters	Counter Acronym	TCA for 15-min bin	TCA for 24-hrs bin
Minimum Round-Trip FD (us)	mB_FD	No	No
Average Round-Trip FD (us)	aB_FD	No	Yes
Maximum Round-Trip FD (us)	xB_FD	Yes	Yes
Minimum Near-End FDV (us)	mN_FDV	No	No
Average Near-End FDV (us)	aN_FDV	No	Yes
Maximum Near-End FDV (us)	xN_FDV	Yes	Yes
Minimum Far-End FDV (us)	mF_FDV	No	No
Average Far-End FDV (us)	aF_FDV	No	Yes
Maximum Far-End FDV (us)	xF_FDV	Yes	Yes

The following table lists the MEF 35 PM counters for LM on 11DPE12A.

Table 15-3 PM Counters defined for pro-active LM on 11DPE12A

PM Counters	Counter Acronym	TCA for 15-min bin/ 24-hrs bin
Near-end High Loss Interval	N_HLI	Yes
Far-end High Loss Interval	F_HLI	Yes
Minimum Near-End FLR	mN_FLR	No
Average Near-End FLR	aN_FLR	Yes
Maximum Near-End FLR	xN_FLR	Yes
Minimum Far-End FLR	mF_FLR	No
Average Far-End FLR	aF_FLR	Yes

Table 15-3 PM Counters defined for pro-active LM on 11DPE12A (continued)

PM Counters	Counter Acronym	TCA for 15-min bin/ 24-hrs bin
Maximum Far-End FLR	xF_FLR	Yes

The following table lists the MEF 35 PM counters for SLM on 11DPE12A.

Table 15-4 PM Counters defined for pro-active SLM on 11DPE12A

PM Counters	Counter Acronym	TCA for 15-min bin/ 24-hrs bin
Near-end High Loss Interval	N_HLI	Yes
Far-end High Loss Interval	F_HLI	Yes
Minimum Near-End FLR (For SLM, only exists in continuous bin)	mN_FLR	No
Average Near-End FLR	aN_FLR	Yes
Maximum Near-End FLR (For SLM, only exists in continuous bin)	xN_FLR	Yes
Minimum Far-End FLR (For SLM, only exists in continuous bin)	mF_FLR	No
Average Far-End FLR	aF_FLR	Yes
Maximum Far-End FLR (For SLM, only exists in continuous bin)	xF_FLR	Yes

The following table lists the MEF 35 PM counters for DM on 11DPE12A.

Table 15-5 PM Counters defined for pro-active DM on 11DPE12A

PM Counters	Counter Acronym	TCA for 15-min bin/ 24-hrs bin
Minimum Round-Trip FD (us)	mB_FD	No
Average Round-Trip FD (us)	aB_FD	Yes
Maximum Round-Trip FD (us)	xB_FD	Yes
Minimum Near-End FDV (us)	mN_FDV	No
Average Near-End FDV (us)	aN_FDV	Yes

Table 15-5 PM Counters defined for pro-active DM on 11DPE12A (continued)

PM Counters	Counter Acronym	TCA for 15-min bin/ 24-hrs bin
Maximum Near-End FDV (us)	xN_FDV	Yes
Minimum Far-End FDV (us)	mF_FDV	No
Average Far-End FDV (us)	aF_FDV	Yes
Maximum Far-End FDV (us)	xF_FDV	Yes
Minimum Near-End FD (us)	mN_FD	No
Average Near-End FD (us)	aN_FD	Yes
Maximum Near-End FD (us)	xN_FD	Yes
Minimum Far-End FD (us)	mF_FD	No
Average Far-End FD (us)	aF_FD	Yes
Maximum Far-End FD (us)	xF_FD	Yes

SAP Ingress Meter/FC counters

The following table lists the new counters per SAP Ingress Meter/Forwarding Class (FC).

Table 15-6 SAP Ingress Meter/FC counters

Counter Acronym	Description
IngressPktsForwarded	Number of frames (In-Profile + Out-of-Profile frames) received in ingress of a SAP and forwarded by this FC meter/policer
IngressOctetsForwarded	Number of octets in frames (In-Profile + Out-of-Profile frames) received in ingress of a SAP and forwarded by this FC meter/policer
IngressPktsDropped	Number of frames dropped by this FC meter/policer (> PIR)
IngressOctetsDropped	Number of octets in frames dropped by this FC meter/policer (> PIR)

Notes:

1. These counters are free-running and do not support binning.

Egress queues counters

The following table lists the counters provided for egress queues, on UNI and NNI.

Table 15-7 Egress queues counters

Counter Acronym	Description	TCA for 15-min bin	TCA for 24hrs bin
PktsForwarded	Number of In-Profile + Out-Of-Profile frames forwarded by a queue on a given port	No	No
OctetsForwarded	Number of octets in In-Profile + Out-Of-Profile frames forwarded by a queue on a given port	No	No
PktsDropped	Number of In-Profile + Out-Of-Profile frames dropped by a queue on a given port	Yes	Yes
OctetsDropped	Number of octets in In-Profile + Out-Of-Profile frames dropped by a queue on a given port	Yes	Yes

LLF per VLAN

In Release 7.0, the LLF feature is extended to LLF enable to SAPs with a VLAN (dot1q encap) for certain hub and spoke applications where a hub-to-spokes fault causes spoke UNIs to shut down. This triggers CE protection to select another hub. To enable LLF on a SAP, there must be exactly one Up MEP configured on the SAP, and its association can have only one remote MEP configured. LLF can only be enabled on one SAP per dot1q-encapsulated port.

Note: The LLF function causes a MEP's port to be shutdown if the MEP detects *Loss of Continuity*, or the received CCM Interface TLV status is not “isUp” from the only peer remote MEP.

Hub to spoke multicast application

In a hub-to-spoke multicast network, a fault on the hub UNI should cause shutdown on the spoke UNIs. Faults on the spoke UNIs should not cause any other UNI to shut down.

This can be accomplished in the following two ways:

- CCM enabled only on the hub MEP

CCM is only required on the hub Up MEP to convey LLF messaging to the spokes. The spoke Up MEPs do not need to send CCM, but do have LLF enabled, and have only the hub MEP configured as a remote MEP. In this case only the direction from hub to spoke is monitored. The hub MEP is configured with no remote MEPs to avoid extraneous CCM loss of continuity alarms.

- CCM enabled on hub and spoke MEPs

CCM enabled on all MEPs provides monitoring in both directions. The spoke MEPs have LLF enabled and have only the hub MEP configured as a remote MEP. Because the other spoke MEPs are not configured as remote MEPs, the spoke MEPs do not process the CCM Interface TLVs from other spokes. As a result, faults on spoke UNIs don't shut down other UNIs, but each spoke MEP will have a persistent MEP-ERR-CCM alarm. The hub MEP does have all of the spoke MEPs configured as remote MEPs so it avoids the extraneous MEP-ERR-CCM alarm, but does not have LLF enabled.

TSoP Smart SFPs

The TSoP Smart SFPs are supported by 11QPE24 and 11QCE12X. They provide transparent SONET/SDH circuit emulation. Although it is called an RMD, the TSoP Smart SFP is inserted in a local port and only managed locally, through an RMD access interface configured on a port.

The user can create a TSoP Smart SFP instance, specifying its rate, on an RMD Access Interface port, if the following conditions are met.

The conditions are:

- the Interface type is 1gbe
- the Interface moduletype is either one of the TSoP types supporting that rate, or auto

The Interface type cannot be changed while a RMD TSoP instance exists.

Alarms generated by TSoP instance interaction

The following alarms are generated if the Interface moduletype was auto and a subsequently inserted SFP is

- not a Smart SFP: Device Not Reachable (DNR)
- non-TSoP Smart SFP: DNR (MAC address incorrect) or WDP (Wrong Device Present) (MAC address correct)
- TSoP Smart SFP with wrong rate: DNR (MAC address incorrect) or WDP (MAC address correct)

Note: The same alarms occur if the Interface moduletype was configured, with the addition of Module Mismatch (MISMATCHMOD) alarm.

The moduletype cannot be changed from a TSoP Smart SFP supporting the rate if the port has a TSoP RMD instance configured.

Ethernet header configuration

- **MAC DA**

The user can configure the unicast Destination MAC Address (DA) for the generated TSoP Ethernet traffic. It must match the MAC address of its peer TSoP Smart SFP.

- **Untagged**

The TSoP Ethernet traffic is always untagged.

- **DA check**

The received DA is always checked against the device MAC address and traffic not matching is dropped.

TSoP header configurations

- **ECID**

The user can configure the Emulated Circuit Identifier (ECID) for transmitted TSoP Ethernet traffic, with default 0.

- **Expected ECID**

The user can configure an expected ECID for received TSoP Ethernet traffic, with default 0.

Note: When received ECID does not match, the packet is dropped and the Missing Packet counter incremented.

- **RTP Payload Type**

The RTP (Real Time transport Protocol) payload type is fixed to 0 and is ignored in received packets.

- **RTP SSRC**

The RTP SSRC (Synchronization SouRCe, a connection identifier) is fixed to 0 and is ignored in received packets.

TSoP encapsulation configuration

- **G-AIS Automatically Generated**

G-AIS (Generalized TDM AIS) is generated automatically based on defect detection. It has no user configuration.

Synchronization

The synchronization mode is fixed to SyncE. For proper operation, both peer TSoP Smart SFPs must have SyncE enabled and synchronized to the same frequency.

Maintenance

The network TDM interface and CES Interworking function are monitored for defects and alarms. Statistics are collected on the internal Ethernet interface and the CES Interworking function Terminal and Facility loopbacks are available on the TDM and Ethernet interfaces.

TSoP per circuit pack limitation

Due to thermal concerns, only a subset of the available SFP ports should be equipped with TSoP SFPs.

For the 11QPE24

- a maximum of twelve TSoP SFPs can be installed on the pack for use in central office. The TSoP SFPs can only be installed in ports C7 - C22.
- a maximum of six TSoP SFPs can be installed on the pack for use outside plant. The TSoP SFPs can only be installed in ports C17 - C22.

For the 11QCE12X

- a maximum of twelve TSoP SFPs can be installed on the pack for use in central office. The TSoP SFPs can be installed in any port.
- a maximum of six TSoP SFPs can be installed on the pack for use outside plant. The TSoP SFPs can be installed in any port.

TPoP/CSoP Smart SFPs - TDM CES

TPoP (Transparent PDH over Packet) and CSoP (Channelized SONET/SDH over Packet) support the E1 and STM-1 channelized TDM CES Smart SFPs. The TPoP SFP can work plug and play without any pre-configuration needed for the user-defined mode. The CSoP can work plug and play without configuration in some cases whereas in other cases, it requires pre-configuration which can be done through the SDM tool.

TPoP/CSoP are supported on the following cards in PSS-4/8/16/16II/32 shelves:

- 11QCE12X
- 11QPE24

TPoP

TPoP stands for Transparent PDH over Packet. TPoP supports Gigabit Ethernet MSA electrical interface and it plugs on the SROS L2 packet card. TPoP also supports Circuit Emulation (CES) function over packet using a structured-agnostic TDM payload mapping as per SAToP (RFC 4553) or MEF-8.

The following features are supported in TPoP SFP:

- SAToP (RFC4553) or MEF-8 unstructured packetizer
- DCR clock recovery using RTP header
- MEF8 Frame header format
- Packetization latency of 1 ms
- Jitter and wander compliant to MEF18, ITU-T G.8261 and ITU-T G.823
- Loss forwarding
- Plug and play: no configuration needed
- Compliant with SFP MSA1

-
- E1 120 Ohm balanced through RJ-45 connector
 - E1 interface complies with ITU-T G.703 (11/2011)
 - Electrical 20-pin MSA interface: GbE, IEEE Std 802.3-2008
 - MSA side in SerDes mode
 - Metal package for lower EMI
 - Operating temperature range: -40°C to 85°C
 - RoHS2 compliant

CSoP

CSoP stands for Channelized SDH over Packet. CSoP supports Gigabit Ethernet MSA electrical interface and it plugs on the SROS L2 packet card. In CSoP, the Circuit Emulation (CES) function converts a fully channelized STM-1 signal into 63 E1 independent signals using SAToP (RFC 4553) or MEF-8 and vice-versa.

The following features are supported in CSoP SFP:

- SAToP (RFC4553) or MEF-8 unstructured packetizer
- DCR clock recovery using RTP header
- 155Mbit/s, S1.1 (15 km) optical interface with optical parameters according to Telcordia GR-253-CORE and ITU-T G.957
- 1310nm FP laser – TDM Application
- LC duplex connector
- Wide dynamic range PIN-PD receiver
- Compliant with SFP MSA1
- DDM SFF-8472 compliant
- Remote DDM
- 63 x E1 SAToP channels into STM-1, interoperable with any E1 SAToP equipment or TPoP Smart SFP
- Loss forwarding
- Electrical 20-pin MSA interface: GbE, IEEE Std 802.3-2008
- Metal package for lower EMI
- Operating temperature range: -40°C to 85°C
- RoHS compliant

Multiprotocol Label Switching - Transport Profile (MPLS-TP)

Overview

Multiprotocol Label Switching (MPLS) is a technology that provides the ability to set up connection-oriented paths over a connectionless network. It does this by assigning labels to service packet traffic to identify the service and the path it takes. Switching is based on these labels, freeing it from any awareness of the protocol transported. It provides its own OAM functions for monitoring and troubleshooting. 1830 supports the Transport Profile subset of MPLS, described in the following sections. For the SROS L2 packet cards (except 11QPE24) it is an operational mode of the card, separate from the Ethernet Provider Bridging "access-uplink" mode.

MPLS Transport Profile (MPLS-TP)

MPLS is used to provide a network layer to support packet transport services. It is desirable that the operation and maintenance of such an MPLS based packet transport network follow operational models typical in traditional optical transport networks (for example, SONET/SDH), by providing additional OAM, survivability and other maintenance functions targeted at that environment.

MPLS-TP defines an IETF-standardized profile of MPLS targeted at transport applications.

Following are the two main objectives of the PSS MPLS-TP:

1. To enable MPLS-TP to be deployed in a transport network and operated in a similar manner to existing transport technologies
2. To enable MPLS-TP to support packet transport services with a similar degree of predictability to that found in existing transport networks

MPLS-TP has a number of high level characteristics in order to meet these objectives:

- It does not modify the MPLS forwarding architecture, which is based on existing pseudowire and LSP constructs. LSPs are point-to-point, bidirectional, and congruent (that is, co-routed and follow the same path in each direction).
- There is no LSP merging.
- OAM, protection and forwarding of data packets operate without IP forwarding support. Static provisioning is used; there is no dependency on dynamic routing or signaling.
- LSP and pseudowire monitoring is only achieved through the use of OAM and does not rely on control plane or routing functions to determine the health of a path.
- MPLS-TP operates in the absence of an IP control plane and IP forwarding of OAM traffic.

In R8.2, this feature is supported on the following cards:

- 11OPE8
- 11QCE12X

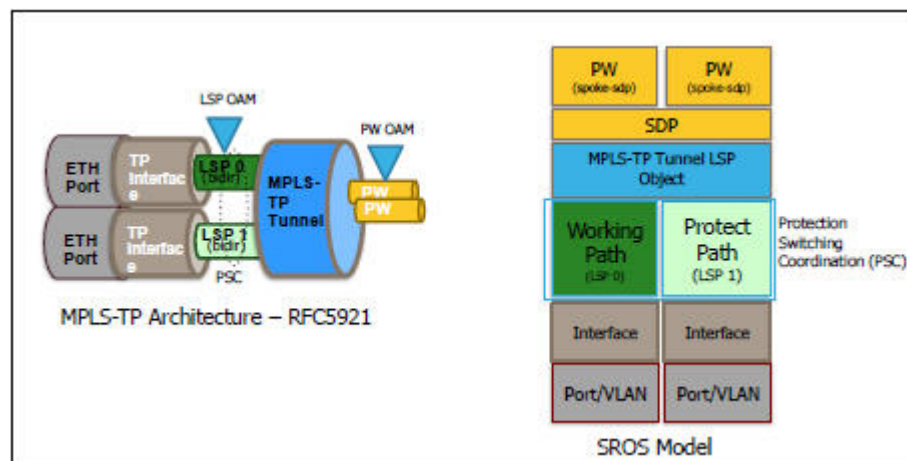
R8.2 supports the following features:

- MPLS-TP on LSPs and PWs with static labels. MPLS-TP is not supported on dynamically signaled LSPs and PWs.
- Static LSPs and PWs on unnumbered interfaces without IP next-hop (from an MPLS perspective).
- PSS supports the role of LER and LSR for static MPLS-TP LSPs, and a T-PE/S-PE for static MPLS-TP PWs.
- MPLS-TP LSP label swap (static LSP label to static LSP label)
- MPLS-TP is supported for EPIPE (Ethernet (Virtual) Private Line) services.
- MPLS-TP OAM
- LSP 1-for-1 Linear protection

MPLS-TP Model

Figure 15-43, “MPLS-TP Model” (p. 15-71) shows a high level functional model for MPLS-TP in PSS. LSP A and LSP B are the working and protect LSPs of an LSP tunnel. These are modelled as the working and protect paths of an MPLS-TP LSP. MPLS-TP OAM runs in-band on each path. 1:1 linear protection coordinates the working and protect paths, using a protection switching coordination protocol (PSC) that runs in-band on each path over a Generic Associated Channel (G-ACh) on each path. Each path uses an MPLS-TP unnumbered (that is, non-IP) interface.

Figure 15-43 MPLS-TP Model



Note: In PSS, all MPLS-TP LSPs are bidirectional co-routed; the forward and backward directions follow the same route (links and nodes) across the network. Both directions are setup, monitored and protected as a single entity. Therefore both ingress and egress directions of the same LSP segment are associated at the LER and LSR and they use the same interface.

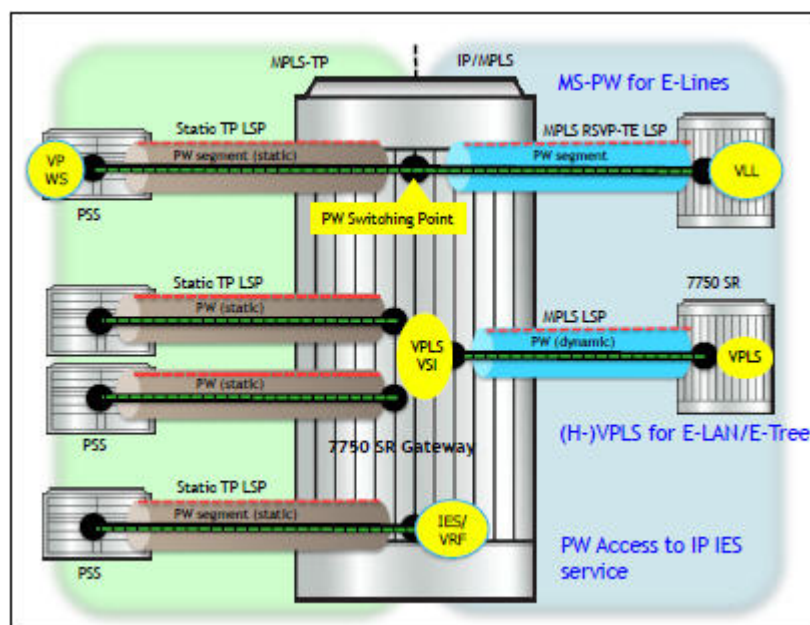
MPLS-TP Provider Edge and Gateway

PSS supports MPLS TP LSPs, and PWs to transport point to point virtual leased line services. The node plays the role of a terminating PE or switching PE for VLLs/Epipe service. T-PE functionality is supported.

VLL Services

Figure 15-44, “VLL services model” (p. 15-72) shows the model for VLL services in an MPLS-TP domain. Static PWs originating in the PSS are transported over static MPLS-TP LSPs. These either terminate on a local SAP, or are switched to another PW segment across the IP/MPLS network.

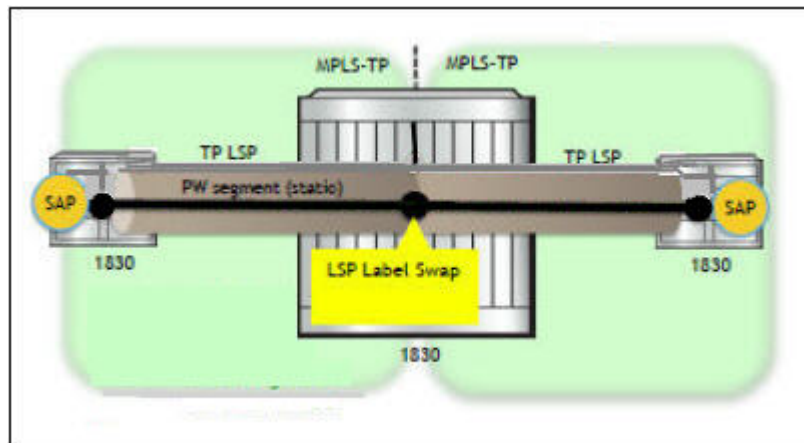
Figure 15-44 VLL services model



LSR Node

PSS swaps a statically configured LSP label on ingress to a statically configured LSP label on egress, to support the LSR node. The graphic below illustrates the MPLS-TP LSR model:

Figure 15-45 MPLS-TP LSR model



MPLS-TP Interfaces

PSS interoperates with MPLS-TP networks in which no IP addressing and routing is used, by configuring an MPLS-TP section layer to a non-IP next hop, bound to a specific port/vlan. This is done using a new interface type, known as an unnumbered MPLS-TP interface. This is an unnumbered interface that allows a broadcast or multicast destination MAC address to be configured.

MPLS-TP Tunnels and LSPs

The 1830 PSS supports the configuration of an MPLS-TP tunnel, containing a working and a protect LSP path. In PSS, a tunnel is referred to as an LSP, while an MPLS-TP LSP is referred to as a path. It is then possible to bind an MPLS-TP tunnel to an SDP.

It is possible to configure MPLS-TP identifiers associated with the LSP, and MPLS-TP OAM parameters on each LSP of a tunnel. MPLS-TP protection is configured for a tunnel at the protect path level. Both protection and OAM configuration is managed through templates, in order to simplify provisioning for large numbers of tunnels.

MPLS-TP on Pseudowires

MPLS-TP is supported on PWs with static labels. The provisioning model supports RFC6370- style PW path identifiers for MPLS-TP PWs.

L2 Services

MPLS-TP PWs is supported on Epipe (VLL) services.

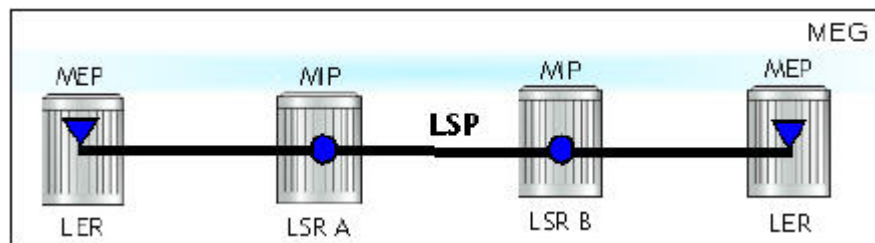
MPLS-TP Maintenance Identifiers

MPLS-TP is designed for use both with and without, a control plane. MPLS-TP therefore specifies a set of identifiers that can be used for objects in either environment. This includes a path and maintenance identifier architecture comprising Node, Interface, PW

and LSP identifiers, Maintenance Entity Groups (MEGs), Maintenance End Points (MEPs) and Maintenance Intermediate Points (MIPs). These identifiers are specified in RFC6370.

MPLS-TP OAM and protection switching operates within a framework that is designed to be similar to existing transport network maintenance architectures. MPLS-TP embraces the concept of maintenance domains to be managed and monitored. In these, Maintenance Entity Group End Points (MEPs) are edges of a maintenance domain. OAM traffic of a maintenance domain must not leak beyond corresponding MEP and so MEPs reside at the end points of LSPs and PWs. Maintenance Intermediate Points (MIPs) define intermediate nodes to be monitored. Maintenance Entity Groups (MEGs) comprise all the MEPs and MIPs on an LSP or PW.

Figure 15-46 MPLS-TP Maintenance Architecture



MPLS-TP OAM

Delivery of services requires that a number of operations occur properly and at different levels in the service delivery model. For example, operations such as the association of packets to a service, must be performed properly in the forwarding plane for the service to function properly. In order to verify that a service is operational, a set of in-band, packet-based Operation, Administration, and Maintenance (OAM) tools is required, with the ability to test each of the individual packet operations.

On-Demand Connectivity Verification (CV) using LSP-Ping

MPLS-TP supports mechanisms for on demand CC/CV as well as route tracing for LSPs and PWs. These are required to enable an operator to test the initial configuration of a transport path, or to assist with fault isolation and diagnosis. On demand CC/CV and route tracing for MPLS-TP is based on LSP-Ping and is described in RFC6426.

The following possible encapsulations are specified in the RFC:

- IP encapsulation, using the same label stack as RFC4379, or encapsulated in the IPv4 GACH channel with a GAL/ACH
- A non-IP encapsulation with GAL/ACH for LSPs and ACH for PWs.

Proactive CC, CV and RDI

Proactive Continuity Check (CC) is used to detect a loss of continuity defect (LOC) between two MEPs in a MEG. Proactive Connectivity Verification (CV) is used to detect an unexpected connectivity defect between two MEPs (for example, mis-merging or misconnection), as well as unexpected connectivity within the MEG with an unexpected MEP.

This feature implements both functions using proactive generation of OAM packets by the source MEP that are processed by the peer sink MEP. CC and CV packets are always sent in-band such that they share fate with user traffic, either on an LSP, PW or section and are used to trigger protection switching mechanisms.

Proactive CC/CV based on bidirectional forwarding detection (BFD) for MPLS-TP is described in RFC6428. BFD packets are sent using operator configurable timers and encapsulated without UDP/IP headers on a standardized G-ACh channel on an LSP or PW. CC packets simply consist of a BFD control packet, while CV packets also include an identifier for the source MEP in order that the sink MEP can detect if it is receiving packets from an incorrect peer MEP, thus indicating a mis-connectivity defect. Other defect types (including period mis-configuration defect) are supported. When a supported defect is detected, an appropriate alarm is generated.

MPLS-TP OAM features

MPLS-TP OAM features include:

- maintenance entities
- proactive protocols for LSPs and PWs
 - BFD for LSP
 - PSC for LSP
 - RDI for LSP
- on-demand protocols for LSPs and PWs
 - ping
 - traceroute
- defects/alarms

A channel is created for OAM PDUs by encapsulating with a special field called Generic Associated Channel Header (G-ACH). A special label, called G-ACH Label (GAL) is placed between the G-ACH and the bottom LSP label to provide an alert that this is an OAM packet.

Note: The GAL is not used for PW OAM.

Maintenance identifiers

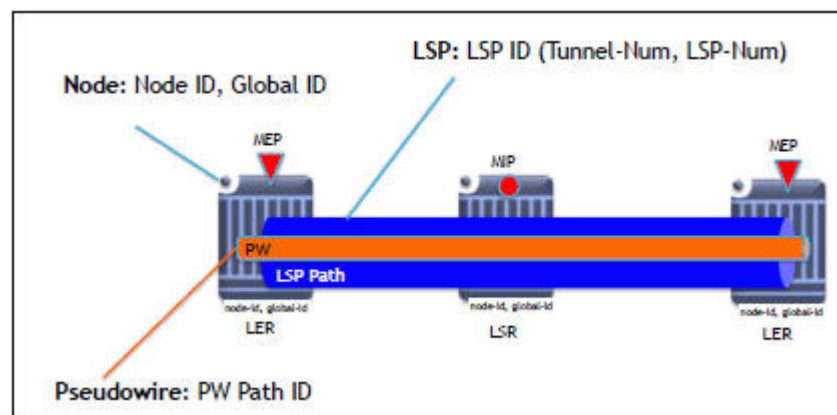
Maintenance identifiers are used to ensure that OAM PDUs propagate to their target Maintenance Entities (MEs), with origin information, to monitor PWs and LSPs.

MPLS-TP OAM supports the following maintenance identifiers:

- **Global_ID:** An optional four-byte prefix to Node_ID that makes it globally unique. The operator's ASN (Autonomous System Number) is recommended; zero means null. If a destination Global_ID is not specified, it defaults to the source Global_ID.
- **Node_ID:** It may be configured in either IPv4 address format or a 32 bit number, which must be unique under the Global_ID.
- **MPLS-TP Tunnel_ID:** The concatenation of two tunnel endpoint identifiers, local followed by remote. Each endpoint identifier is the concatenation of [Global_ID]::Node_ID::Tunnel_Num. The range of Tunnel_Num is 1 - 61440 and is independent at each end for flexibility.
- **LSP_ID:** The concatenation of MPLS-TP Tunnel_ID::LSP_Num, although the ordering of local and remote parts is not significant. The range of LSP_Num is 1 - 65535.
- **PW_Path_ID:** The concatenation of AGI::SAII::TAII where the source and target AII (Attachment Individual ID) consists of the [Global_ID]::Node_ID::AC_ID of each end. The AC_ID (Attachment Circuit ID) is a 32-bit number. The AGI (Attachment Group ID) is a 32-bit number (zero means null).
- **MEG_ID:** For LSPs this is the LSP_ID, where the tunnel endpoint identifiers are in local than remote order. For PWs this is the PW_Path_ID.
- **MEP_ID:** For LSPs this is an endpoint part of the LSP_ID, with the LSP_Num suffix. For PWs this is AGI::[Global_ID]::Node_ID::AC_ID for each end.
- **MIP_ID:** Only one per node, this is [Global_ID]::Node_ID::0.

The graphic below illustrates the Operations and Maintenance: MPLS-TP Identifiers.

Figure 15-47 Operations and Maintenance: MPLS-TP Identifiers



Maintenance Entities

- **Maintenance Entity Group (MEG):** For MPLS-TP, an MEG is a logical entity consisting of the MEPs and MIPs of an LSP or of a PW. These MPLS-TP MEGs are not explicitly created and have no configurable attributes and there is only one "maintenance level".
- **Maintenance Entity group endPoint (MEP):** A MEP can be configured at each end of an LSP, for the purpose of enabling BFD. It need not be configured for on-demand OAM. For an LSP an OAM template can be applied and BFD enabled. Additionally for a protection LSP, a protection template can be applied. For PWs, an MEP is not configured but is implied by the creation of the PW-Path_ID.

MPLS-TP MEPs operate independently from CFM MEPs.

- **Maintenance Intermediate Point (MIP):** One MIP per LSP or PW per node (not per interface) is supported. MIPS are not configured explicitly; the creation of a path-id (static LSP FEC) and PW-path-ID (static PW FEC), at a transit-path LSR or S-PE, respectively, implicitly creates and enables the MIP to reply. See the following graphic for example.

Figure 15-48 MPLS-TP LSR Maintenance Entities

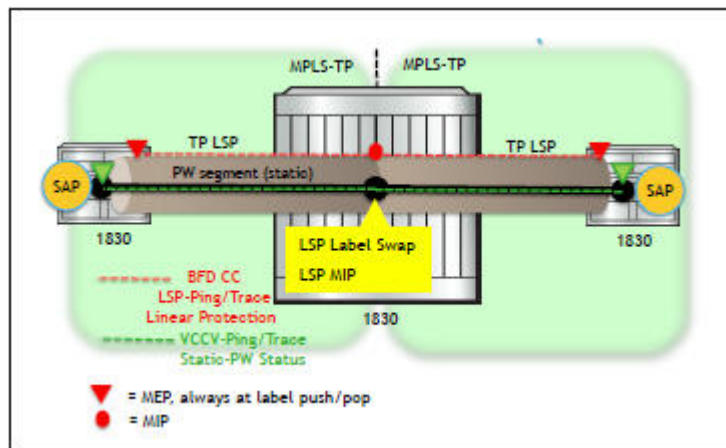
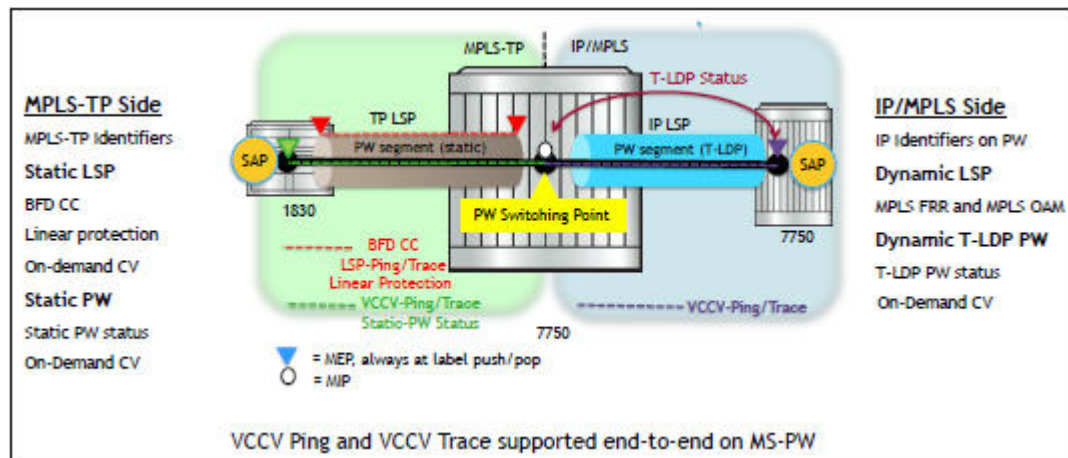


Figure 15-49 PW switching to extend VLL between -TP and -IP networks

MPLS-TP protection

MPLS-TP protection is bidirectional and it operates end-to-end. PSS supports linear 1:1 protection of MPLS-TP LSPs as defined in RFC 6378.

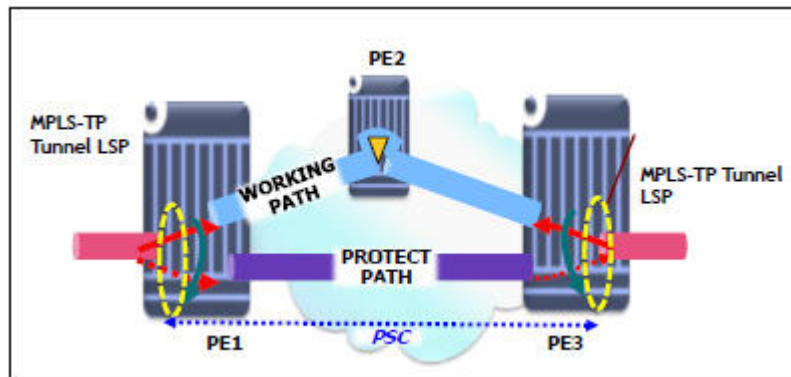
MPLS-TP protection is supported on the 11OPE8 and 11QCE12X cards.

Note: Linear MPLS-TP protection applies only to LSPs in the current release.

MPLS-TP LSP protection

Figure 15-50, “1:1 LSP linear protection” (p. 15-79) shows 1:1 LSP linear protection. BFD runs on both the working and protect LSPs as a defect detection mechanism. The working and protect LSP paths together form an MPLS-TP Tunnel. MPLS-TP linear protection is used to select the LSP that is used at any given time for the MPLS-TP Tunnel.

This is supported edge-to-edge on an LSP, between two LERs, where normal traffic is transported either on the working LSP or on the protection LSP using a logical selector bridge at the source of the protected LSP.

Figure 15-50 1:1 LSP linear protection**Single phase switching**

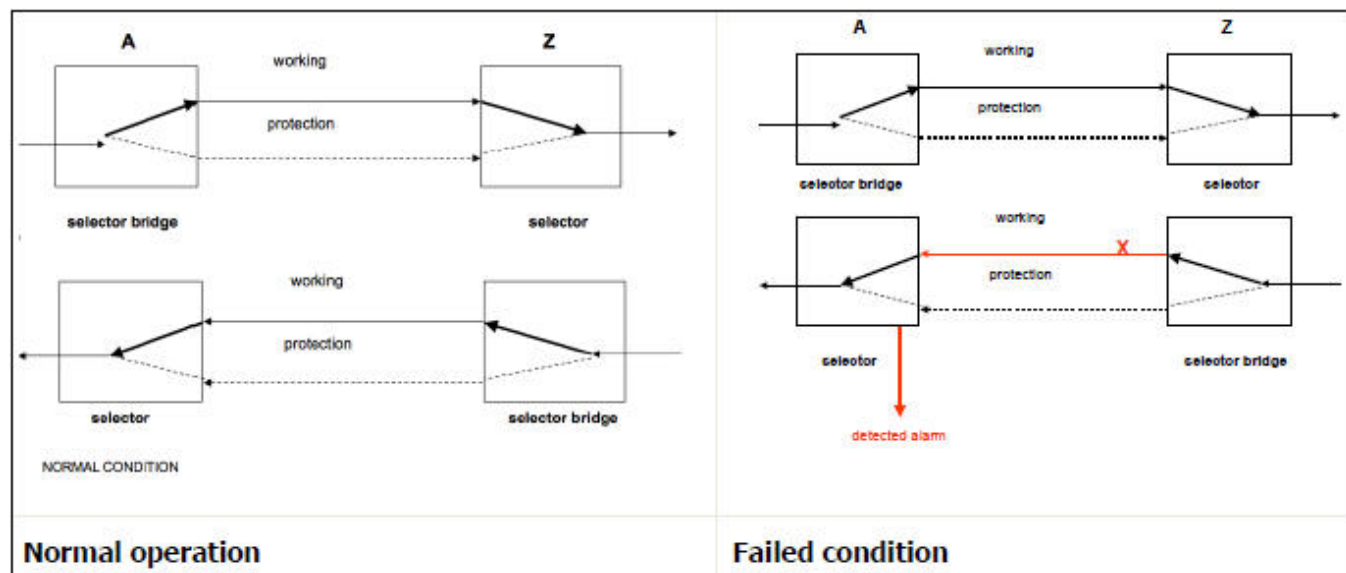
At the LER sink of the LSP Tunnel, the LSP path that carries the traffic is selected, and that path becomes the active LSP. A Protection Switching Coordination (PSC) protocol coordinates between the source and sink bridge, to identify the LSP path to be used as the active path.

The PSC protocol is always carried on a G-ACh on the protection LSP.

Bidirectional operation

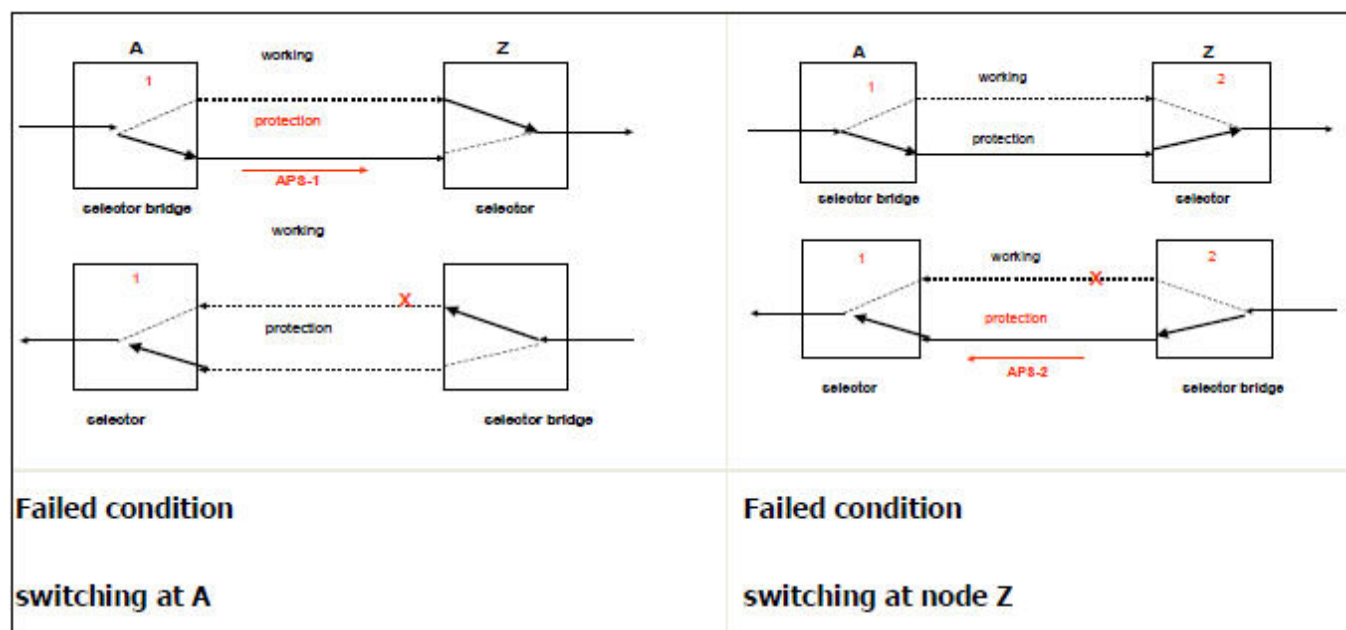
The 1:1 linear protection is bidirectional, and can be configured as non-revertive or revertive. For non-revertive, the service will not switch back to the working LSP path when the PSC switch requests end, while for revertive configurations, the service always returns back to the working LSP path when the switch requests end.

Figure 15-51 Bidirectional operation

**Bidirectional operation (Failed)**

In normal condition, the user data packets are sent on the working path in both the directions, from A to Z and Z to A. A defect in the direction of transmission from node Z to node A impacts the working connection Z to A, and this in turn initiates the detection of a defect at the node A.

Figure 15-52 Bidirectional operation (Failed)



In the case of unidirectional PSC protocol, protection switching is initiated and the selector bridge at node A is switched to the protection connection A to Z. The selector at node A switches to the protection connection Z to A. The PSC packet, sent from node A to node Z, requests a protection switch to node Z.

Node Z validates the priority of the protection switch request, and then the selector at node Z is switched to the protection connection A to Z and the selector bridge at the node Z is switched to protection connection Z to A. The PSC packet, sent from node Z to node A, is used to acknowledge and inform node A about the switching.

BFD CC OAM packets are inserted on both working and protection paths to detect defects on these paths.

Note: BFD CC OAM packets are sent regardless of whether the selected path is the currently active path.

Note: Linear protection targets 50 ms as the protection time, but this does not include the defect detection time, or the configurable hold-off time. The hold-off time starts when a defect condition is declared and runs for a non-resettable period. When the timer expires, protection switching is initiated if a defect condition is still present at this point.

Ethernet OAM

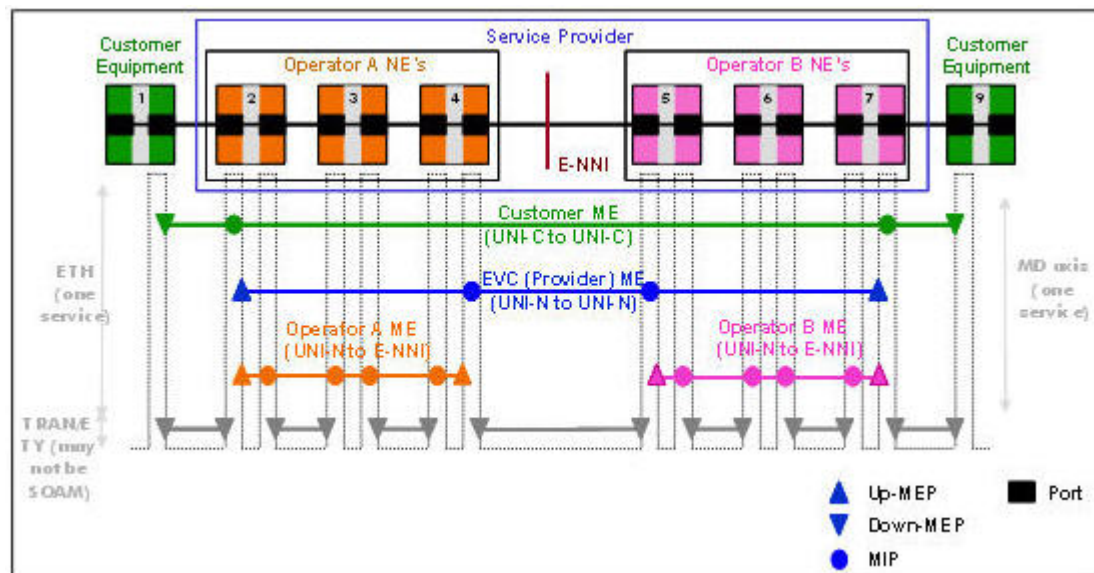
Overview

Ethernet OAM provides functionalities to detect, verify and isolate connectivity failures in Virtual Bridged Local Area Networks through Continuity Check, LoopBack and Link Trace protocols. These functionalities can be used in network operated by multiple independent organizations, each with restricted access to each other equipment.

11DPE12E supports only the CCM function in current release. 11DPE12A supports, the Connectivity Check Message (CCM), LoopBack (LB), RDI, and CSF functions.

The network administrator is informed about the failure in the connections, based on the reception of Continuity Check or by the user. The administrator can then initiate LoopBack or Link Trace accordingly to determine and isolate the fault condition.

Figure 15-53 Ethernet service OAM Reference model



The CFM information is conveyed in Slow Protocol frames called CFM Protocol Data Units (CFM PDU). The CFM PDU contains the appropriate control and status information that is used to detect, verify, and isolate faults. It also contains information for path discovery in CFM-enabled links. The CFM PDUs are processed and passed by the entities configured in the Bridge port based on the Maintenance Domain Level to which that entity belongs.

Fault detection

CFM uses the Continuity Check protocol to detect both connectivity failures and unintended connectivity between service instances. Each MEP periodically transmits a multicast Connectivity Check Message (CCM) announcing the identity of the MEP and